



# BRIGHT MINDS

## Q & A SERIES



January 2022

## **Developing Proactive, Responsive, and Ethical Artificial Intelligence Policies**

Joyce Hunter, ICIT Executive Director

**ICIT's Bright Minds Q&A Series**

# Developing Proactive, Responsive, and Ethical Artificial Intelligence Policies

---

With Joyce Hunter, ICIT Executive Director

**January 2022**

Copyright 2022 Institute for Critical Infrastructure Technology. Except for (1) brief quotations used in media coverage of this publication, (2) links to the [www.icitech.org](http://www.icitech.org) website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

## **About This ICIT Bright Mind Q&A:**

In continued support of our mission to cultivate a cybersecurity renaissance that will improve the resiliency of our nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders, ICIT has embarked on a journey to hold candid interviews with some of the brightest minds in national security, cybersecurity, and technology. Our goal is to share their knowledge and insights with our community to shed light on solutions to the technology, policy, and human challenges facing our community. We hope that their words will motivate, educate, and inspire you to confront your organizations' challenges.

## **About ICIT:**

The Institute for Critical Infrastructure Technology (ICIT) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

## **About this Bright Mind:**

Joyce Hunter is the Executive Director of the Institute for Critical Infrastructure Technology (ICIT). Before joining ICIT, she served as the Interim CIO and Deputy CIO of the US Department of Agriculture and held other senior leadership roles within the federal government, Lotus Development Corp, Lawson Software, and Computer Sciences Corporation (CSC). Joyce has managed multi-billion-dollar IT budgets and established or led several data governance and PMO initiatives. She understands how to communicate with and across diverse communities and forge relationships that enable those stakeholders to succeed. She regularly uses these skills in both her TEDx talks and publications.

Joyce has a BA from Villanova University and an MBA in Marketing from the University of Pennsylvania, Wharton School of Business. She holds certificates in Emotional Intelligence, Design Thinking, Technology Business Management (TBM), and Scaled Agile Framework (SAFe). She sits on multiple industry boards and is active in several philanthropies focused on advancing STEM and Data Science education for underserved and underrepresented youth.

## **About Ethical Artificial Intelligence**

Ethical AI development ensures that security and privacy considerations are implemented into the lifecycle of machine learning, artificial intelligence, and algorithmic systems and in the collection of the data necessary to leverage those technologies, such that no risk is transferred to, or harm inflicted on the data subjects and such that the bias inherent in the solution is minimized.

## How can nations be more responsive to emerging threats and the potential applications of artificial intelligence and machine learning?

### Joyce Hunter:

Nations should be cognizant of the realities and the potential benefits of artificial intelligence and machine learning, but they should also be aware of how threat actors could weaponize it. It has much to do with being proactive instead of just reactive. For example, artificial intelligence can help predict emerging threats by analyzing trends. It can also help to pen test critical systems for undiscovered vulnerabilities, and it can automate some cybersecurity tasks to help alleviate the burden on information security teams. Meanwhile, adversaries may leverage the same artificial intelligence and machine learning to probe for exploitable vulnerabilities, mutate malware, and glean valuable insights from stolen data sets, such as in the case of the 79.8 million SF-86 forms stolen during the 2015 OPM breach.

So, we need to be proactive in such a way that we are not running around like chickens with our heads cut off. In my experience, people are in denial because they thought it wouldn't happen to them. Instead of jumping into a practiced incident response plan, they become paralyzed by shock. Cybersecurity incidents are not a matter of if it will happen. It's a matter of what you do when it happens.

---

## What kinds of changes are necessary to shift towards proactive action at a national level?

### Joyce Hunter:

That is a challenging question because it's all about culture, and as the saying goes, "culture eats strategy for breakfast.." In my opinion, it is more like culture eats strategy for breakfast, lunch, and dinner.

The first step in shifting culture is demystifying the implications and realities of AI. Many people think of AI-based on what they see in movies and television. They believe that it's all this big mysterious thing like in 2001 space Odyssey, War Games, or the Terminator. But we are far off from Hal 9000 or Skynet. We are at a point where an algorithm can analyze structured or unstructured data according to user specifications to ascertain trends, make predictions, or determine correlations.

---

**Is there a need for AI to be regulated? If yes, do you have any recommendations?**

**Joyce Hunter:**

Potentially but at the moment, we aren't doing enough to make sure that there are no unintended consequences when you're developing the algorithm. There needs to be more cooperation and collaboration between the public and private sectors.

One of my most significant recommendations is that we need to address the level of diversity underlying the concept of AI. When you develop the code for AI, you can't have only a homogeneous group developing the code because their biases will propagate throughout the algorithm. We need to increase the diversity of AI development teams to mitigate harmful biases and improve actionable results. We need to start educating young people to select AI, programming, or data science so that we can have decent representation in those areas.

---

**What collaborative steps can nations take to achieve an AI-inspired, responsive framework to forestall future economic erosion and protect global supply chains from disruption?**

**Joyce Hunter:**

With AI, we could correlate factors that might impact supply chains, preempt events that might result in socioeconomic erosion, increase collaboration between the public and private sectors and international partners. Unfortunately, we must start at the beginning. You can't run before you walk or before you crawl. It has to be the other way around. And before we start applying AI asymmetrically or haphazardly, we should focus on developing a framework and standards that meet the needs of the public and private sectors. For comparison, in healthcare, we have domestic and international standards that dictate what organizations can do and how they can do it. Once we begin to establish benchmarks and baselines, we can begin to increase international collaboration to scale the framework to protect global supply chains.

We can begin that process by forming committees, drawing stakeholders together, and initiating discussions about standards, how we will educate k-12 students, college students, young professionals, and the current workforce. Even if they don't know anything about artificial intelligence or blockchain, it just takes the three C's: communication, collaboration, and coordination.

---

**What form could a responsive and ethical framework take? Are there specific issues or needs that should be addressed?**

**Joyce Hunter:**

In a sense, we need to prioritize codifying ethical standards before development. We need to be careful to understand what should and should not be automated and why. Similarly, we need to govern better what data is collected, how it is anonymized, whether it can be transferred, and how long it should be retained.

Everything should not be automated. There still needs to be some human factor somewhere along the line. We need to determine which roles and responsibilities in data collection and processing are delegated to humans and AI systems. We should be more cognizant of the potential risks collected information might pose to our data subjects if compromised. We need to increase our national dialogue from a privacy and security perspective to one that prioritizes the security and privacy of the citizens and the data subjects and does not exploit or harm individuals, even when the data is collected ethically or legally, it's about the citizens.

Currently, by default, many organizations start on a very slippery slope by trying to collect as much data as possible with minimal regard for all the potential future harms and implications. Risk to the data subjects or systems is not considered because the risk is not assumed by the organization collecting, processing, or transferring the data. It is seen as a revenue stream, and any potential risk or breach is viewed more as a legal issue than an ethical one. As systems become more integrated and more data is collected, transferred, processed, combined, and retained, the need to consider ethical regulations increases as the risk of harm increases. With AI arguably in its infancy, we have a diminishing window of time to institute ethical regulations, frameworks, standards, and governance right the first time around; and it is already an uphill battle with major tech companies.

I don't have all the answers for what would constitute an ethical or actionable framework, and giving you all my thoughts could take up many more pages. So instead, let me pivot back to a previous point and say that a step in the right direction would be to consider the perspectives of all the diverse group of stakeholders, including the data subjects, tech companies, privacy advocates, security leaders, from all backgrounds and walks of life, and kickstart a constructive dialogue focused around developing actionable standards and codes of conduct.

---



**You mentioned the need to focus on the foundation or basics as a community to maximize AI's long-term potential. What would you consider core fundamentals or bare basics regarding education and workforce development?**

**Joyce Hunter:**

We should place greater focus on initiatives that improve critical thinking and diversity of race, background, age, and perspective. Contrary to the myth, progress doesn't come from isolated genius or lightning in a vacuum. Innovation comes from collaboration, communication, and coordination. The journey, the path, and who are invited are as important as the end result. Progress is an iterative process that develops from the cycle of articulating and addressing stakeholder needs. It isn't just about identifying a problem or assuming that we (the developers) know the best solution. We need to focus on those three C's. After we improve on those and apply them to the development process on an individual level, we can address how we scale those processes to an organizational, state, national, or international level.

---

**How critical is engagement with the younger generations (K-12 and University) on topics related to cybersecurity and emerging technologies?**

**Joyce Hunter:**

Our young people are our greatest resource (and, for some, our greatest frustration). We are reaching a point where most young people were not born before the internet and are accustomed to interconnectivity and technology by default. If we teach them the responsible ways to engage with technology and we instill critical thinking and ethical application in them at the proper developmental stages, then we can preempt many of the cybersecurity and cyber-hygiene pitfalls that we encounter with our workforce.

I was the Deputy CIO at the Department of Agriculture, so let me frame it this way: by 2030, we are projected to have 8.5 billion people to feed globally, and by 2050, we could have as many as 9.7 billion. Global populations are growing, supply chains are becoming more international, and critical systems are becoming more interconnected. Over the same period, public and private infrastructures are becoming more integrated and more dependent on emerging technologies that scale to meet demands. If we do not take advantage of our younger generations and teach them to crawl, walk, and run when it comes to emerging technologies, then we will be in more trouble than we are now.

---

## Are there challenges specifically related to the existing workforce?

### Joyce Hunter:

Cybersecurity culture is all about trends, and unfortunately, the data consistently shows that most people just clicked through training as fast as possible. They don't pay attention to materials or retain the information in the long term. When I was at the Department of Agriculture, you were automatically sent to training if you failed three questions. People didn't like it, and they didn't like me for doing it, but they couldn't do anything else because I required their computer to be shut down until they went through the cyber training.

In a way, it's like a driving test; if you study that information, then you could pass the test. But I don't want people to just click through it to pass because then, after it leaves their short-term memory, they could put others at risk. We need to be more creative with our development, engagement, and delivery of cybersecurity and cyber-hygiene training so that personnel retain information in the long term and act responsibly by default. Gamification, automating some of the burdens, and other novel methods might be a promising direction.

---

## Are there any final thoughts you would like to impart to our audience?

### Joyce Hunter:

At a time when the country is grappling with systemic bias in core societal institutions, we need technology to reduce health disparities, not exacerbate them. We have long known that AI algorithms trained with data that do not represent the whole population often perform worse for underrepresented groups.

It's not just healthcare; AI has begun to play the role of a trained expert in other high-stakes domains. AI tools help judges with sentencing decisions, redirect the focus of law enforcement, and suggest to bank officials whether to approve a loan application. Before algorithms become an integral part of high-stakes decisions that can enhance or derail the lives of everyday citizens, we must understand and mitigate embedded biases.

To ensure that the algorithms of tomorrow are not just powerful but fair, we must build the technical, regulatory, economic, and privacy infrastructure to deliver the large and diverse data required to train these algorithms. We can no longer move forward blindly, building and deploying tools with whatever data happens to be available, dazzled by a veneer of digital gloss and promises of progress, and then lament the "unforeseeable consequences." The consequences may be foreseeable. Still, they do not have to be inevitable.

---