ISSUE 2 | VOL. 22 | FEBRUARY 2024

www.issa.org

ISSA

ADVANCING CYBER SECURITY, EMPOWERING PROFESSIONALS

8 CYBER-TECH OBSERVATIONS OF 2023 AND WHAT IT MEANS FOR 2024

PRESIDENTS LETTER REWIND

TRAVEL BACK IN TIME TO FEBRUARY 2004 WITH A LETTER FROM FORMER PRESIDENT DAVID M. CULLINANE

CRYPTIC CURMUDGEON

CISSP Course on Social Media

CRYPTO CORNER

The Ultimate Computer?

PYTHON PROGRAMMING

Numerical Analysis/Machine Learning Series

CONTENTS

INFORMATION SYSTEMS SECURITY ASSOCIATION
40
40 YEARS STRONG

Dr. Shawn P. Murray

International President

Hello Everyone, welcome to February!

As we enter the second month of the new year, I want to share with you some exciting things we are doing. First, welcome SFE Partners as the new management company led by our new Executive Director, Jennifer Hunt. Jen and her team bring a plethora of association and event management experience to the table. You will see her and the ISSA operations team leading event planning initiatives, engaging members and chapters as well as transitioning to more effective and efficient operational continuity for your association. You will see them out and about, please say hello!

Your International Board of Directors is engaged as well. We will be meeting in Clearwater Florida for the next in person board meeting collocated with the next Cyber Executive Forum. If you are a chapter leader, you can request to attend! We are also gearing up for RSA, Blackhat and will move the annual awards gala to Q4 in Boston. Look for additional details on the website and in marketing materials, as members receive registration discounts for many of the larger conferences. This allows members to receive additional value for their membership!

I have had several conversations with many chapter leaders recently regarding various topics and to gain insight about what our members are doing in their community. Mentorship seems to be a very popular topic so we will be highlighting what some chapters are doing so that others can create similar programs for their chapters as well. Be sure to check out the Apprenticeship Internship and Mentorship (AIM) committee to gain access to additional resources as they become available.

Can you believe that ISSA has been around since 1984? I was a senior in high school and computers were just becoming a thing! As we commemorate 40 years of excellence in Information Security, it is with great pride and reflection that we revisit pivotal moments in our organization's history. Over the next 12-18 months you will begin to see a number of flashbacks from the last 40 years of the ISSA both here in our Journal, as well as across our various digital and social channels.

In this spirit, we are pleased to include a special President's Letter from 2004 in the upcoming edition of the ISSA Journal. This letter, penned during a time of significant growth and evolution in the cybersecurity landscape, serves as a testament to the enduring commitment of our members and the visionary leadership that has propelled the ISSA forward. By revisiting this letter, we not only honor our rich legacy but also reaffirm our dedication to advancing the field of information security through knowledge sharing, collaboration, and innovation. As we look back with gratitude, let us also look forward with renewed determination to continue our mission of promoting cybersecurity excellence for the next 40 years and beyond.

Regards,
Dr. Shawn P. Murray, President
ISSA International Board of Directors

President Letter Rewind

February 2004

David M. Cullinane, CPP, CISSP

Dear Fellow Members,

As usual, it has been a busy month. The CISO Executive Forum we held in New York city was a resounding success. We are busy establishing the forum as an ongoing membership category for the ISSA. If you are the person responsible for information security at your organization, we encourage you to check out this new membership designed specifically to meet your needs as a CISO. Go to http://ciso.issa.org for more information.

As I mentioned in last month's letter, there is a great deal of activity going on in US legislative circles to develop legislation relative to "corporate governance" of information security and other aspects of the National Cyber Security Strategy. Mike Rasmussen has been representing the ISSA on Congressman Putnam's "Corporate Information Security Working Group." I have been representing the ISSA on Congressman Putnam's "Corporate Information Security Working Group." I have been representing you on the DHS Coporate Governance Task Force and was asked last week to co-chair the Compliance & Verification Subcommittee of that Task Force. Space doesn't permit providing the details of all the activity here, but we will be communicating what is going on through ISSA e-news.

The more important result of my comments in last month's letter was an e-mail from one of our members in Germany - Alex Eble. Alex asked an excellent question: *"Why are you only doing this in the US?* The simple answer is that we have been able to identify who we need to talk to in the US. If you or any of your colleagues can help us identify who we should be talking to in other parts of the world, we will be more than happy to approach them and offer the services of the ISSA, the world's largest association of information security professionals, as they deal with difficult issues about information security, identity theft and privacy.

I am sure you have noticed the dramatic changes since *Password* became *The ISSA Journal.* The changes have been the hard work of a number of people, including Stephen Scharf, Greg Dunne, Jenny Kasza (the editor), and Denise Rockhill (the publisher). Among the many activities they have been involved in has been creating an editorial advisory board for *The ISSA Journal* - people who can help us continue to build *The ISSA Journal* into the most valuable publication you read. The editorial advisory board for *The ISSA Journal* is complete. It's a mix of professionals from different sectors in the industry who are excited to help shape the future of the publication. We welcome their contributions to the ISSA. Look for more on this topic in an upcoming issue of *The ISSA Journal.*

Also, please be sure to read our new column, Point/Counterpoint, in this month's issue. The first question for debate is whether exploitation code should be released to the public. You will see professional opinions both for and against doing so. readers should feel free to send their opinions to theeditor.org. We may publish some of those responses in future issues of *The ISSA Journal.*

Last month I announced that we were splitting the Marketing and Communications board positions into two separate positions and creating a new position - VP of Vendor Relations. While it was the board's intention to have these two positions included in the upcoming elections, it turned out that the election process (which is run independently by the past president of the ISSA) was too far along to make the changes in time for the upcoming election. Consequently, after consultation with the board, I am naming Stephen Scharf to fill the position of VP of Communications and Jim Reavis as the VP of Vendor Relations. Both have been making major contributions in those areas without the benefit of any recognition for all the work they have been doing. We welcome them to the board and look to their continued assistance in making the ISSA more valuable to you.

With all the activity that has been going on, I've neglected to mention several new chapters that have recently joined the ISSA. With my sincere apologies for the oversight, I would now like to formally welcome the Greater Spokane, Washington Chapter (established 10/13/03), the Brasil-SP Chapter (established 10/14/03), the Buffalo Niagara, New York Chapter (established 11/21/03), the Hong Kong Chapter (established 12/17/03), and the Central Alabama Chapter (established 12/19/03). We keep growing and continue to become a truly global association. Welcome to all of you, and be sure to let me know how we can make the ISSA more responsive to your needs.

Best Regards,
Dave

Jack Freund

Editor, ISSA Journal NC Charlotte Metro Chapter

Welcome to the February 2024 issue of the ISSA Journal!

As we continue unraveling the intricate world of cybersecurity, we're excited to present an array of compelling articles and insights that promise to shape your understanding of the industry.

In our feature article, "Eight AI Cyber-Tech Trends of 2023 and What it Means for 2024," penned by cybersecurity experts Jeremy Swenson and Matthew Versaggi, we delve deep into the transformative power of artificial intelligence in the realm of cybersecurity. This article serves as a beacon for the cybersecurity community, offering astute analysis and projections for 2024 based on the pivotal trends of 2023.

But that's not all! Pamela Fusco shares her invaluable expertise in "How to Build and Present a Budget that Gets Board Approval." In a world where financial contraints often hinder security efforts, Pam provides actionable strategies to navigate budgetary challenges and secure the resources necessary to fortify your organization's cyber defenses. This piece was transcribed by our very own Debra Christofferson from a talk that Pam presented recently at the Women in Security Executive Speaker Series.

Additionally, our book reviews section, curated by the discerning eye of Jay Carson, brings you insightful critiques of the last cybersecurity literature. Carson's reviews provide a glimpse into the knowledge that can be gleaned from these books, helping you make informed choices about your reading list.

In an era where cyber threats continue to evolve and proliferate, staying ahead of the curve is imperative. The ISSA Journal remains your steadfast companion in this endeavor, offering cutting-edge insights and expert perspectives. We trust you'll find this month's content as illuminating and thought-provoking as we do.

Thank you for your unwavering support, and we eagerly anticipate sharing more enlightening content with you in the coming months.

The information and articles in this magazine have not been subjected to any formal testing by Information Systems Security Association Inc. The implementation, use, and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, are the responsibility of the reader.

Articles and information will be presented as technically correct as possible and to the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry, and/or changes/enhancements to hardware or software components.

The opinions expressed by the authors who contribute to the ISSA Journal are their own and do not necessarily reflect the official policy of ISSA. Articles may by submitted by members of ISSA. The articles should be within the scope of information systems security and should be a subject of interest to the members and based on the author's experience. Please call or write for more information. Upon publication, all letters, stories, and articles become the property of ISSA and may be distributed to, and used by, all of its members.

ISSA is a not-for-profit, independent corporation and is not owned in whole or in part by any manufacturer of software or hardware. All corporate information security professionals are welcome to join ISSA. For information on joining ISSA and for membership rates, see www.issa.org.

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.

NOW INDEXED WITH EBSCO

Service Directory

Website
webmaster@issa.org
Nick Cefalo

Chapter Relations
chapter@issa.org
Joe Moroney & Amy Velez

Member Relations
memberservices@issa.org
Mamen Garcia & Nick Radar

Executive Director
execdir@issa.org
Jennifer Hunt

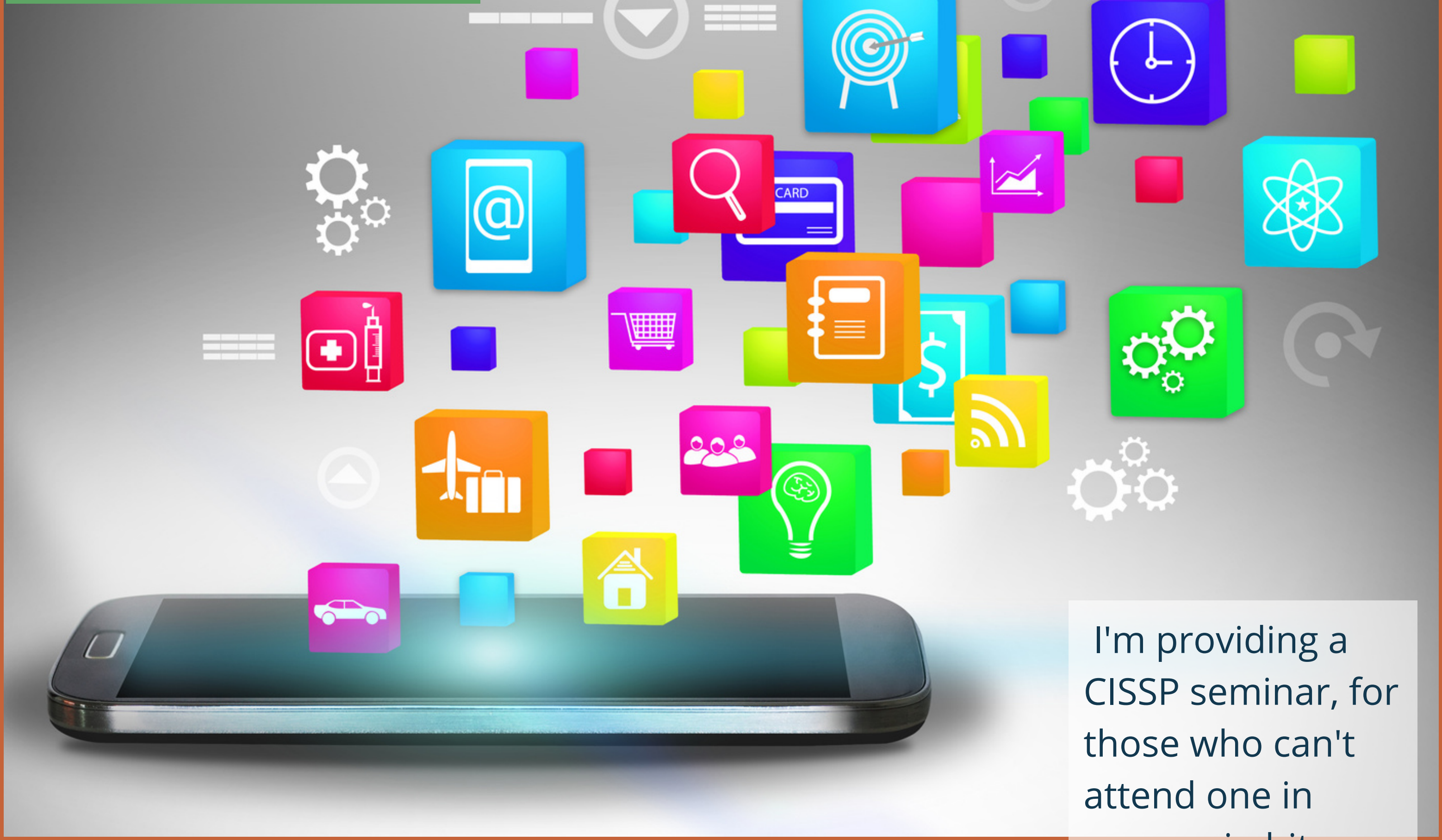
Sponsorships
sponsorships@issa.org
Lisa O'Connell

Journal Advertising
sponsorships@issa.org
Phil D'Agostino

ABOUT ISSA

ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure.

The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.



CISSP Course on Social Media

I'm providing a CISSP seminar, for those who can't attend one in person, in bits and pieces.

Study the CISSP on your coffee break! (I realized that that is one advantage of this weird, social media posting regime ...)

As some of you may have noticed, in my recent bios, I'm providing a CISSP seminar, for those who can't attend one in person, in bits and pieces.

The CISSP is the Certified Information Systems Security Professional designation, the professional level certification for security in the field of computer, communications, and information systems, and the people who work in them. It is, of course, the people who write the exam and get certified.

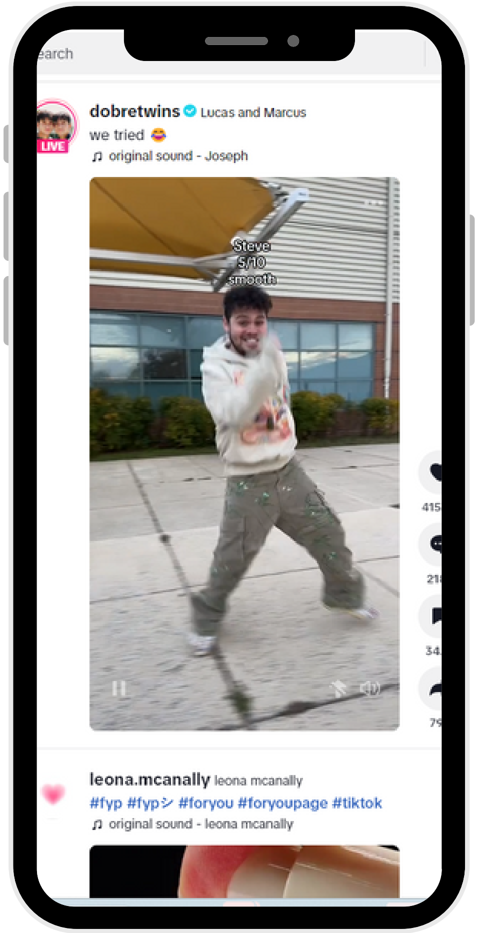
I have facilitated such preparation seminars, and contributed material for such seminars, for multiple organizations, including (ISC)^2 (the International Information Systems Security Certification Consortium, the maintainer of the CISSP certification and examinations), for more than twenty years. I have taught on six continents.

The preparation seminars are not cheap. And they're not always available. And they're not all of the same quality, nor are the people facilitating such seminars. So, now that I am, ostensibly, retired, I figure it's time to do my bit in aid of the profession. So, I'm conducting a seminar, for free, in a rather unusual way.

I'm doing this seminar while I'm walking around town, in little video segments, that I can then upload to various of social media platforms. Since TikTok seems to be very popular right now, I'm including TikTok, and it's TikTok that seems to be the limiting factor. TikTok has a ten-minute maximum limit for video clips, so I'm keeping the individual video clips under ten minutes. So, there are going to be hundreds of such clips, to cover the full forty hours of the material in the seminar. I figure it will take at least a year, and possibly two, to get the whole seminar done this way, but, once it's up, then all of you lot can use it, in any way you like, forever. Or, at least until social media, as an activity and as various companies, falls out of favor, and these various systems go by the board. Anyway, this seminar will be available for a while.

I started this out as an experiment. The experiment isn't over yet and I'm not quite sure what the results are or are likely to be. People are watching the videos, although trying to get details about how many people are watching the videos is not easy. The various platforms have different ways of recording, or reporting, the views and reactions to the videos that I'm posting, and it's not consistent in terms of figuring out how people are reacting.

It's been interesting doing the seminar with no feedback or reactions. On the one hand, I feel that I can say whatever I want, and can add extra stories without regard to the time of day, or how people will react to me taking up extra time. But, on the other hand, I am not sure how well I am doing at explaining things, and whether people understand all the points that I'm trying to make. Nobody, so far, is taking any opportunities to clarify any points that I'm making.


earch
LIVE
dobretwins Lucas and Marcus
we tried 😂
♫ original sound - Joseph
Steve
5/10
smooth
415
21
34
79
leona.mcanally leona mcanally
#fyp #fyp #foryou #foryoupage #tiktok
♫ original sound - leona mcanally

TikTok has a ten-minute maximum limit for video clips, so I'm keeping the individual video clips under ten minutes. So, there are going to be hundreds of such clips, to cover the full forty hours of the material in the seminar.

I find it interesting that I'm not getting more response to a seminar which, after all, can cost up to $5,000 to take, and which I am providing for free. On the other hand, I haven't yet completely finished all of the material and so some may be waiting until it is complete. It'll take me a few months yet to get all the pieces in place, but, even so, I was surprised that people are not taking the opportunity to take the seminar, and to use the extra time that is afforded for studying.

I'm posting the clips to YouTube, where my channel is, apparently, known as @TheRslade or TheRslade, and which I consider to be the central repository and most organized, and I've created a playlist for it https://www.youtube.com/playlist?list=PLUuvftvRsRv7D5PiHIULhhd9M032ej4_i , as well as the aforementioned TikTok https://www.tiktok.com/@robertmslade/video/7200511642847825158 or https://www.tiktok.com/@robertmslade/ , Facebook https://www.facebook.com/rslade/ (yes, I *do* have an account, but I only use it for emergency backup posting, so don't try and contact me there), LinkeDin https://ca.linkedin.com/in/rslade , and Instagram https://www.instagram.com/robertmslade/ .

So far, all of the introduction [CISSP 0.xx], the security management domain [CISSP 1.xx] , and access control [CISSP 2.xx, security architecture [CISSP 3.xx], applications security [CISSP 4.xx], and cryptology [CISSP 5.xx] are complete. I'm currently starting into physical security [CISSP 6.xx]. (I expect I'll be into BCP [CISSP 7.xx] by the time you read this.)

Of course, I expect a number of people will simply follow along on the video clips, and do their preparation that way. However, I hope that some of you will take the opportunity to form study groups, watch the video clips together, and discuss them. Study groups, formed and operating over a period of time, allow you to prepare much better for the exam, and to bounce ideas off each other in order to more fully understand the principles of security, and form the appropriate attitudes to the security profession, which is really what the examination is trying to assess in any case.

Links and more details are at https://fibrecookery.blogspot.com/2023/02/cissp-seminar-free.html

About the Author

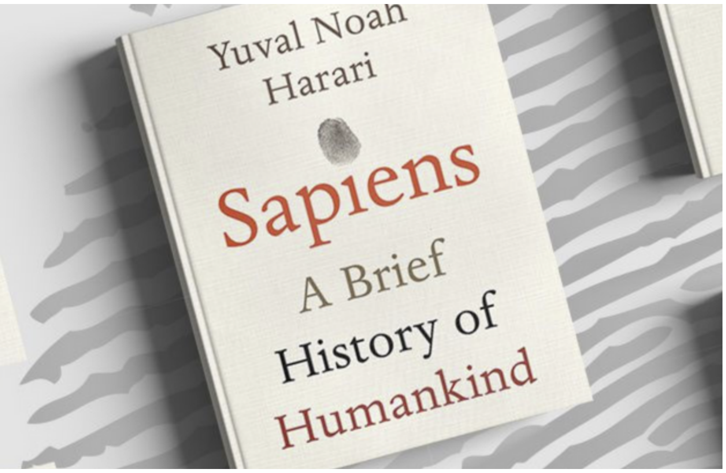
By Robert Slade

Robert Slade talks a lot. If you want, you can (virtually) accompany him on his daily walk (and prep for your CISSP exam) at https://fibrecookery.blogspot.com/2023/02/cissp-seminar-free.html It is next to impossible to get him to take bio-writing seriously, but you can try at the-usual-suspect@outlook.com

The Ultimate Computer?

In the 1968 *Star Trek* episode "The Ultimate Computer," when Captain Kirk was replaced by the M-5 Multitronic Unit in Star Fleet war games, things start off well. So well, that another Star Fleet officer jokingly referred to Kirk as "Captain Dunsel," possibly a 23rd-century reference to the ancient (by then) ChatGPT. Eventually chaos ensued, and we eventually learned that it was caused by the designer of the M-5 basing it's operation on how humans think, resulting in nothing more than a really, really fast human equivalent, with all of the issues that you might expect to come with that. That might be where artificial intelligence (AI) is headed, but it could get even weirder. Much weirder.

Human psychology is a set of evolved behaviors that tend to increase our chances of survival and reproduction. Some of these have led to possibly undesirable consequences. As Yuval Noah Harari noted in his book *Sapiens*, humans ruthlessly wiped out many indigenous species as they colonized the planet over the past millennia. And we are not just tough on other species. As Dale Peterson and Richard Wrangham noted in their book *Demonic Males: Apes and the Origins of Human Violence*, humans are one of just a handful of species that engage in organized, lethal violence against members of their own species. It's pretty clear that our psychology has been defined by a very particular history and has resulted in something that's tailored to solve a very particular set of problems. A big part of that is what we think of as "intelligence," and it is a set of behaviors that helps us solve problems that might interfere with us surviving and reproducing. Both for good and bad.



But AI is probably being trained for an entirely different set of goals. It's hard to tell exactly what those goals are at this point and what interesting emergent properties we might get from systems designed to pursue those goals, but it's probably safe to assume that far-future AI isn't going to be pursuing the same goals that humans do. It's probably not going to be optimizing its behavior to increase its chances of survival and reproduction, and the result of that is probably going to be something that is about as non-human as you can get. We share the common goals of survival and reproduction with all other forms of life: dogs, cats, trees, ants, bacteria, etc. So it shouldn't be too surprising if we end up having more in common with ants and trees than we do with any form of AI. Unless we make the AI think just like people do. And that's pretty much what we seem to be trying to do, and I think it just might end up giving us an early version of the M-5 Multitronic Unit.

And as Douglas R. Hofstadter suggested in Gödel, Escher, Bach, we should expect AI-based on human behavior to have some of the same quirks that we do. You might want your AI-based assistant to help you plan a two-week trip to Europe, but your AI-based assistant might really prefer to play a game of chess instead, and come up with a long list of reasons why you should play chess now and worry about planning the trip later. Just like a person might do.

AI might actually have the potential to do great things, but I suspect that we're artificially crippling it in some cases. Instead of finding patterns in data, we're training AI to find the patterns that we want it to find in data.

> AI might actually have the potential to do great things, but I suspect that we're artificially crippling it in some cases.

There are lots of things that are true, but many people don't want to be true. And when AI systems find these patterns, the systems are often modified so that the undesirable patterns are not found, after all. To use some of that symbolic logic that I had in a general education class in college many years ago, we have systems that find *P*, but we're then training them to find *NOT P*, even though the data supports *P*. And, like I learned in that logic class, from a false premise you can prove absolutely anything.

A reasonable definition of "intelligence" probably includes the ability to find patterns in data. If you add two odd numbers you always get an even number. That sort of thing. But when we intentionally avoid finding patterns in data because they make us uncomfortable, that suggests to me that we might not be as intelligent as we like to think we are. And that's probably not something that even the best AI can help us with.

About the Author

By Luther Martin

ISSA Member, Silicon Valley Chapter

Luther Martin has survived over 30 years in the information security industry, during which time he has probably been responsible for most of the failed attempts at humor in the ISSA Journal. You can reach him at lwmarti@gmail.com.

Book Reviews

By William J. (Jay) Carson
Aka 'Dad'
The Cyber Librarian
ISSA Member, Colorado Springs Chapter

Disclaimer: These are the author's subjective opinions, and do not necessarily reflect the opinions of any organization or other individual. A human prepared this article, with assistance from Microsoft Editor and Grammarly.

I have a terrific group of colleagues as reviewers who generously make great improvements to these articles. I greatly respect, but do not always follow their advice. For example, I am told by one to delete the tables of contents' reviews, but another reviewer finds that the best part. I am told the comments about public library availability are unnecessary, but I am trying encourage professional reading by ISSA members where paying $50 for a book means less food on the table. I am also told to give more of my own thoughts. That comment I will follow this time! Sorry!

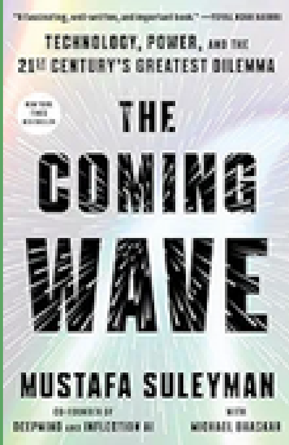
We are all star-struck with idols to some degree, often in the entertainment or athletics industries. My idols are really smart people who have proven they know their topics and write well about them. Both Mustafa Suleyman and Anu Bradford fit the category.

Current readers of the Artificial Intelligence business must know of Mustafa Suleyman. To say he is a major leader in artificial intelligence development is a great understatement. His reasoned positivism gives me hope, and you might have recently seen him on CNN's *Fareed Zakaria GPS.* And then there is Anu Bradford.

When I was studying for my CIPP/E, I read in English the entire GDPR, including the recitals. It is tough reading, but fortunately, I spent years in my past life reading NATO documents. Frankly, the GDPR is like reading serious works by Yoda the Jedia Master. Every long sentence seems to end in a vowel! So I was expecting something similar from a (initially) European-trained law professor.

In contrast, Anu Bradford's writing is refreshingly clear. It is quite serious, mind you, but she gets to the point. I do not personally know her, but I am a major fan! To prove it, I intend to read her earlier acclaimed book, *The Brussels Effect: How the European Union Rules the World.*

01. Suleyman, Mustafa. *The Coming Wave: Technology, Power, and the 21st Century's Greatest Dilemma.* Crown (2023)



Sound Bite: Do not lose sight of the benefits of AI and synthetic biology while recognizing the harms.

Opinion on Primary Audience: World

This book will inspire you to deal with the many challenges of our technological future. Mustafa Suleyman believes in humanity, and our capacity to find and harness AI to find solutions to challenges in a wide variety of recent technologies, including synthetic biology. The 'wave' of modern technologies looks overpowering. We can be knocked down by it, or we can surf it.

The Author

Mustafa Suleyman's credentials are more in the 'school of hard knocks.' He is an Oxford dropout, but was a Founder of DeepMind, a VP at Google, and for the last two years a Founder of Inflection AI. Call it at least 14 years of experience in cyber leadership, especially AI. Other AI books I have read reference him as a major leader. I note the book jacket and title page say, "with Michael Bhaskar." Mr. Bhaskar has an MA from Oxford and is an experienced writer and publisher with several books to his credit.

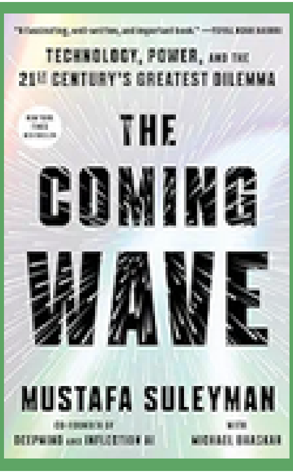
The Metadata

A ***2023*** publishing date! The online ordering cost, including shipping, is under $25, a third less with an e-reader. The hardcover book is over 300 pages, including notes pages. My local public library system has multiple copies, but an extensive 'hold' list. Public library availability is noted for those like me who try to keep costs down.

I took a one-page sample of the text to analyze for readability. Using a Wikipedia article about the Flesch-Kinkaid Readability Test, the readability is high school level. There was under 5% passive voice in my sample. I sense the expert hand of Mr. Bhaskar in making the book so readable. This article is about 6% passive voice, for comparison.

Table of Contents (abbreviated/modified and annotated in bold font (inside parenthesis) by me)

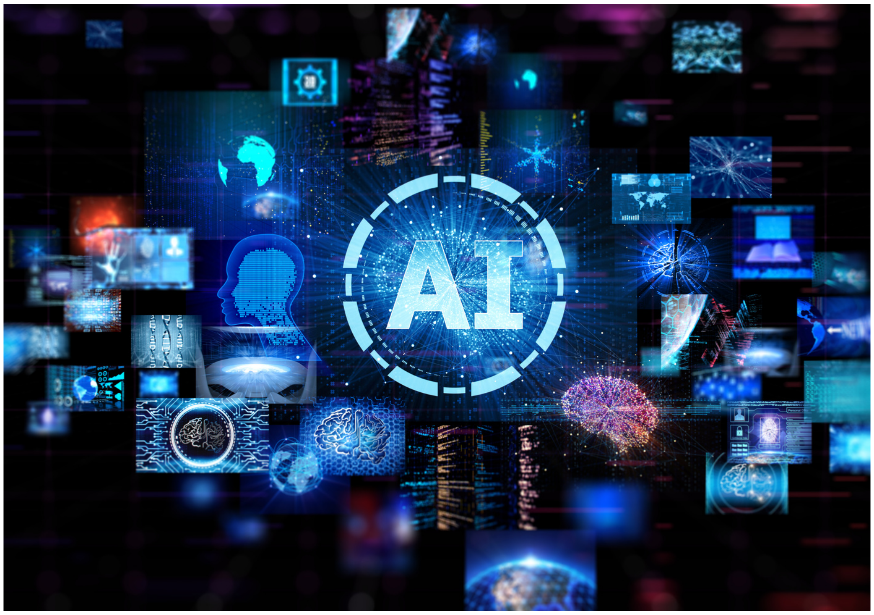
Suleyman, Mustafa. *The Coming Wave: Technology, Power, and the 21st Century's Greatest Dilemma.* Crown (2023)


TECHNOLOGY, POWER, AND THE 21ST CENTURY'S GREATEST DILEMMA
THE COMING WAVE
MUSTAFA SULEYMAN
CO-FOUNDER OF DEEPMIND AND INFLECTION AI
WITH MICHAEL BHASKAR

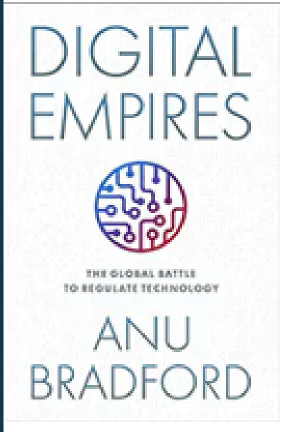
Part II The Next Wave
4 The Technology of Intelligence **(Good AI history here)**
5 The Technology of Life **(Good bioengineering history here)**
6 The Wider Wave **(AI will impact everything)**
7 Four Features Of The Coming Wave
(#1 AI is an asymmetric force compared with past innovations)
#2 AI is not just growing, it is accelerating
#3 AI spreads everywhere
#4 Compared to AI, we are like gorillas in a zoo. Physically stronger, but not as smart)
8 Unstoppable Incentives **(We have no choice - deal with it)**

Part III States of Failure
9 The Grand Bargain
10 Fragility Amplifiers **(Cybersecurity people - read this!)**
11 The Future of Nations **(Wish Kissinger was here to comment)**
12 The Dilemma **(Even if we could shut AI down, can we afford to stagnate?)**

Part IV Through the Wave
13 Containment Must Be Possible
14 Ten Steps Toward Containment **(below are the author's ten)**
#1 Technical Safety
#2 Audits
#3 Choke Points
#4 Makers
#5 Businesses
#6 Government
#7 Alliances
#8 Culture
#9 Movements
#10 Coherence



02. Bradford, Anu. *Digital Empires: The Global Battle to Regulate Technology. Oxford University Press (2023)*


DIGITAL EMPIRES

THE GLOBAL BATTLE TO REGULATE TECHNOLOGY

ANU BRADFORD

Sound Bite: Two major points: 1) Defense against China's growing authoritarian power requires international teamwork. 2) Tech companies in the US market-driven model have enormous power, not always used wisely.

Opinion on Primary Audience: Anyone with a need to understand global economies in the digital age. Especially important for international-level cyber leaders.

When you see a video of an international cyber and/or privacy lecture, you routinely see the lecturer in front of shelves of privacy books. Look at the books. If *Digital Empires* is not there, make a mental question mark on the lecturer's topic currency.

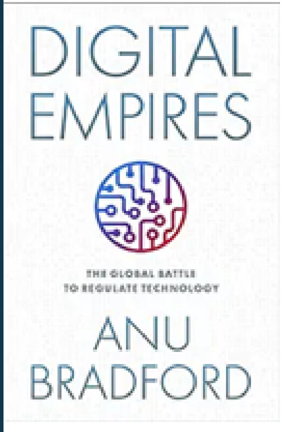
I am seeing a lot of books on the China domination threat and will be reviewing some in later articles. These books clearly state the challenge, but their solutions seem to lead to economic or actual warfare. Professor Bradford offers a workable solution. It is for the U.S. and the EU to team up and blend the market-driven digital approach of the U.S. with the EU rights-based approach. Together, they make a more powerful example to the world.

I worry that no one seeing this book in a bookstore or library will pick it up as a potential read. The hardcover edition is thick, the print is small, and there are no pictures. It is a good personal defense weapon for a bar fight, assuming you take books to bars. I do, but everyone thinks I am strange.

Not reading it would be a crying shame, for it is a fine book, well worthwhile for cybersecurity and privacy leaders. The reason for the heft is over 150 pages of meticulous notes. The body of the book is readable, enjoyable, and if you aspire to global corporate leadership, important.

You will need to understand her terminology of horizontal conflict - governmental system against government system, and vertical conflict - governmental system against its own and foreign-owned digital corporations. Daring to mildly criticize a superbly credentialled author, I found the book a bit too supportive toward the European digital management model, not surprising with the author's legal and early training background, and her familiarity with the European management systems. She is listed in Wikipedia as a Finnish American, and her first degree was from a Finnish university. If that sounds presumptive on my part, let me clearly state she is not above criticizing the European model for a lack of innovation results compared to the U.S. market model. My caution is because I just finished listening to Walter Isaacson's *Elon Musk* and wonder if Mr. Musk would find the European individual rights-based world confining.

Bradford, Anu. *Digital Empires: The Global Battle to Regulate Technology. Oxford University Press (2023)*



While I am certainly **not** a fan of Mr. Musk, he does get things done.

The Author
Professor Bradford has wonderful academic and writing credentials for her subject. In addition to her Law master's degree from the University of Helsinki, she has her master's degree and JD from Harvard. She currently holds a prestigious International Law professorship at Columbia Law School, where she has taught for over 11 years. She speaks four European languages in addition to English. This is her second book.

The Metadata
A ***2023*** publishing date! The online ordering cost, including shipping, is under $35. You can cut that cost by half if you use e-reader. The hardcover version is about 550 pages including notes. My public library has no copies. Loan, but do not give away this book. If you ever go for a privacy certification, I consider it essential background reading.

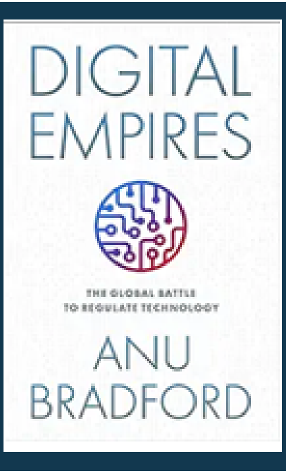
I took a one-page sample of the text to analyze for readability. Using a Wikipedia article about the Flesch-Kinkaid Readability Test, the writing level and style measurement is graduate school level. There was around 50% passive voice in my sample, but the author keeps it interesting with examples. This article is about 6% passive voice, for comparison.

Table of Contents (abbreviated/modified and annotated in bold font (inside parenthesis) by me)

Part I Digital Empires

Part II Imperial Rivalries

Bradford, Anu. *Digital Empires: The Global Battle to Regulate Technology. Oxford University Press (2023)*



Part III The Expansion of Empires
7 The Waning Global Influence of American Techno-Libertarianism **(Big surprise - authoritarian governments find America a dangerous influence on their populations)**
8 Exporting China's Digital Authoritarianism through Infrastructure **(Exactly 'how' China is taking control of a long-term basis, through appeals to authoritarian governments and infrastructure deals)**
9 Globalizing European Digital Rights through Regulatory Power **(A reasonable solution to balance China's growing power)**

Happy Reading!

PS - If you have a book you want me to read & review, please use the email address in my bio to let me know!

For next month's reviews, I got two terrific suggestions from people I follow on LinkedIn. Ben Rothke recommended:

Schneier, Bruce. *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back.* New York: W.W. Norton & Company, 2023.

Robert Metzger recommended:
McLaughlin, Michael G., and William Holstein. *Battlefield Cyber: How China and Russia Are Undermining Our Democracy and National Security.* Washington, DC. Rowman & Littlefield, 2023.

Additional sources used in the article:

1. https://en.wikipedia.org/wiki/Anu_Bradford
2. https://en.wikipedia.org/wiki/Mustafa_Suleyman
3. LinkedIn profiles for authors listed, where available.
4. https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests

About the Author

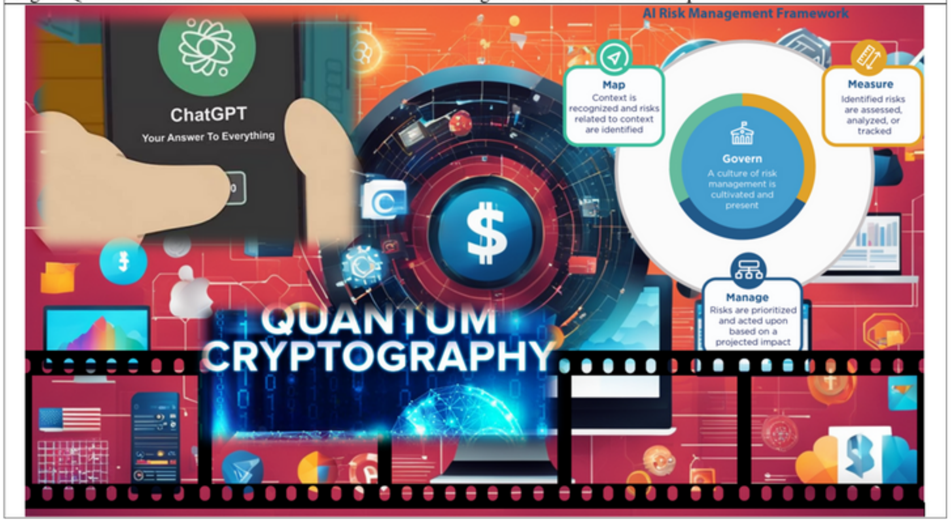
William J. (Jay) Carson, ISSA Senior Member, ISSA 2020 Volunteer of the Year, and a past ISSA-Colorado Springs Executive Vice President. He is the part-time 'Cyber Librarian' of Semper Sec, LLC. Holding Security+ and CIPP/E certifications, he is a former high school math/science teacher, civil servant, contractor, and retired USAF Lieutenant Colonel. He can be reached at Runningjay51@gmail.com.

EIGHT ARTIFICIAL INTELLIGENCE (AI) CYBER-TECH TRENDS OF 2023 AND WHAT IT MEANS FOR 2024

By Jeremy Swenson & Matthew Versaggi

1. **The Complex Ethics of Artificial Intelligence (AI) Swarms Policy Makers and Industry Resulting in New Frameworks**
2. **ChatGPT and Other Artificial Intelligence (AI) Tools Have Huge Security Risk**
3. **Artificial Intelligence (AI) Powered Threat Detection Has Improved Analytics**
4. **The Zero-Trust Security Model Becomes More Orchestrated via Artificial Intelligence (AI)**
5. **Quantum-Safe Cryptography Ripens**
6. **Artificial Intelligence (AI) Streamline Cloud Security Posture Management (CSPM)**
7. **Artificial Intelligence (AI) Driven Threat Response Ability Advances**
8. **Artificial Intelligence (AI) Enhanced Authentication Arrives**

Fig. 1. Quantum ChatGPT Growth Plus NIST AI Risk Management Framework Mashup [1, 2, 3].


AI Risk Management Framework
ChatGPT
Your Answer To Everything
Map
Context is recognized and risks related to context are identified
Measure
Identified risks are assessed, analyzed, or tracked
Govern
A culture of risk management is cultivated and present
Manage
Risks are prioritized and acted upon based on a projected impact
QUANTUM CRYPTOGRAPHY

This year is unique since policy makers and business leaders grew concerned with artificial intelligence (AI) ethics, disinformation morphed, AI had hyper growth including connections to increased crypto money laundering via splitting / mixing. Impressively, AI cyber tools became more capable in the areas of zero-trust orchestration, cloud security posture management (CSPM), threat response via improved machine learning, quantum-safe cryptography ripened, authentication made real time monitoring advancements, while some hype remains. Moreover, the mass resignation / gig economy (remote work) remained a large part of the catalyst for all of these trends.

Every year we like to research and comment on the most impactful security technology and business happenings from the prior year. This year is unique since policy makers and business leaders grew concerned with artificial intelligence (AI) ethics [4], disinformation morphed, AI had hyper growth [5], crypto money laundering via splitting / mixing grew [6], AI cyber tools became more capable - while the mass resignation / gig economy remained a large part of the catalyst for all of these trends. By August 2023 ChatGPT reached 1.43 billion website visits per month and about 180.5 million registered users [7]. This even attracted many non-technical naysayers.

Impressively, the platform was only nine months old then and just turned a year old in November [8]. These numbers for AI tools like ChatGPT are going to continue to grow in many sectors at exponential rates. As a result, the below trends and considerations are likely to significantly impact government, education, high-tech, startups, and large enterprises in big and small ways, albeit with some surprises.

1. The Complex Ethics of Artificial Intelligence (AI) Swarms Policy Makers and Industry Resulting in New Frameworks:

The ethical use of artificial intelligence (AI) as a conceptual and increasingly practical dilemma has gained a lot of media attention and research in the last few years by those philosophy (ethics, privacy), politics (public policy), academia (concepts and principles), and economics (trade policy and patents) - all who have weighed in heavily. As a result, we find this space is beginning to mature. Sovereign nations (The USA, EU, and elsewhere globally) have developed and socialized ethical policies and frameworks [9, 10]. While major corporations motivated by profit are all devising their own ethical vehicles and structures - often taking a legalistic view first [11].

Moreover, The World Economic Forum (WEF) has weighed in on this matter in collaboration with PricewaterhouseCoopers (PWC) [12]. All of this contributes to the accelerated pace of maturity of this area in general. The result is the establishment of shared conceptual viewpoints, early-stage security frameworks, accepted policies, guidelines, and governance structures to support the evolution of artificial intelligence (AI) in ethical ways.

For example, the Department of Defense (DOD) has formally adopted five principles for the ethical development of artificial intelligence capabilities as follows [13].

1. Responsible
2. Equitable
3. Traceable
4. Reliable
5. Governable

Traceable and governable seem to be the most clear and important principles, while equitable and responsible seem gray at best and they could be deemphasized in a heightened war time context. The latter two echo the corporate social responsibility (CSR) efforts found more often in the private sector.

The WEF via PWC has issued its Nine AI Ethical Principles for organizations to follow [14], and The Office of the Director of National Intelligence (ODNI) has released their Framework for AI Ethics [15]. Importantly, The National Institute For Standards in Technology (NIST) has released their AI Risk Management Framework as outlined in Fig. 2. and 3. They also released a playbook to support its implementation and have hosted several working sessions discussing it with industry which we attended virtually [16]. It seems the mapping aspect could take you down many AI rabbit holes, some unforeseen – inferring complex risk. Mapping also impacts how you measure and manage. None of this is fully clear and much of it will change as ethical AI governance matures.

Fig. 2. NIST AI Risk Management Framework (AI RMF) 1.0 [17].

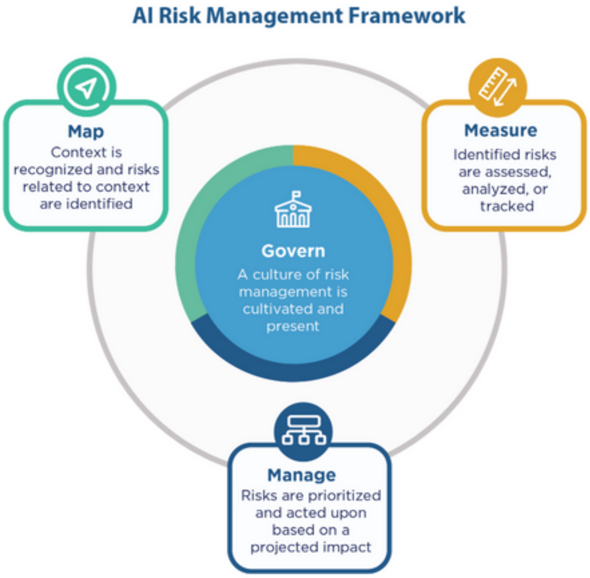
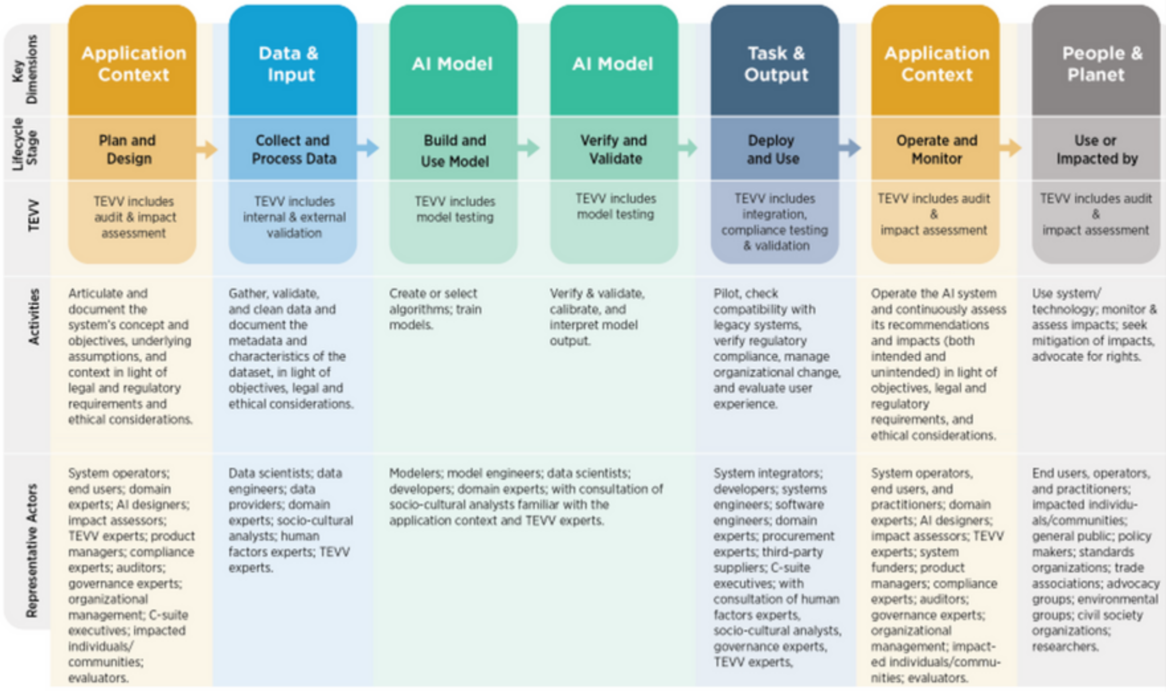

AI Risk Management Framework
Map
Context is recognized and risks related to context are identified
Measure
Identified risks are assessed, analyzed, or tracked
Govern
A culture of risk management is cultivated and present
Manage
Risks are prioritized and acted upon based on a projected impact

Fig. 3. NIST AI Risk Management Framework: Actors Across AI Lifecycle Stages (AI RMF) 1.0 [18].



Key Dimensions	Application Context	Data & Input	AI Model	AI Model	Task & Output	Application Context	People & Planet
Lifecycle Stage	Plan and Design	Collect and Process Data	Build and Use Model	Verify and Validate	Deploy and Use	Operate and Monitor	Use or Impacted by
TEVV	TEVV includes audit & impact assessment	TEVV includes internal & external validation	TEVV includes model testing	TEVV includes model testing	TEVV includes integration, compliance testing & validation	TEVV includes audit & impact assessment	TEVV includes audit & impact assessment
Activities	Articulate and document the system's concept and objectives, underlying assumptions, and context in light of legal and regulatory requirements and ethical considerations.	Gather, validate, and clean data and document the metadata and characteristics of the dataset, in light of objectives, legal and ethical considerations.	Create or select algorithms; train models.	Verify & validate, calibrate, and interpret model output.	Pilot, check compatibility with legacy systems, verify regulatory compliance, manage organizational change, and evaluate user experience.	Operate the AI system and continuously assess its recommendations and impacts (both intended and unintended) in light of objectives, legal and regulatory requirements, and ethical considerations.	Use system/ technology; monitor & assess impacts; seek mitigation of impacts, advocate for rights.
Representative Actors	System operators; end users; domain experts; AI designers; impact assessors; TEVV experts; product managers; compliance experts; auditors; governance experts; organizational management; C-suite executives; impacted individuals/ communities; evaluators.	Data scientists; data engineers; data providers; domain experts; socio-cultural analysts; human factors experts; TEVV experts.	Modelers; model engineers; data scientists; developers; domain experts; with consultation of socio-cultural analysts familiar with the application context and TEVV experts.		System integrators; developers; systems engineers; software engineers; domain experts; procurement experts; third-party suppliers; C-suite executives; with consultation of human factors experts, socio-cultural analysts, governance experts, TEVV experts,	System operators, end users, and practitioners; domain experts; AI designers; impact assessors; TEVV experts; system funders; product managers; compliance experts; auditors; governance experts; organizational management; impacted individuals/communities; evaluators.	End users, operators, and practitioners; impacted individuals/communities; general public; policy makers; standards organizations; trade associations; advocacy groups; environmental groups; civil society organizations; researchers.

The actors in Fig. 3. cover a wide swath of spaces where artificial intelligence (AI) plays, and appropriately so as AI is considered a GPT (general purpose technology) like electricity, rubber, and the like – where it can be applied ubiquitously in our lives [19]. This infers cognitive technology, digital reality, ambient experiences, autonomous vehicles and drones, quantum computing, distributed ledgers, and robotics to name a few. These were all prior to the emergence of generative AI on the scene which will likely put these vehicles to the test much earlier than expected. Yet all of these can be mapped across the AI lifecycle stages in Fig. 3. to clarify the activities, actors, dimensions, and if it gets to build, then more scrutiny will need to be applied.

Scrutiny can come in the form of DevSecOps but that is extremely hard to do with such exponentially massive AI code datasets required by the learning models, at least at this point. Moreover, we are not sure if any AI ethics framework does justice to quality assurance (QA) and secure coding best practices much at this point. However, the above two NIST figures at least clarify relationships, flows, inputs and outputs, but all of this will need to be greatly customized to an organization to have any teeth. We imagine those use cases will come out of future NIST working sessions with industry.

Lastly, the most crucial factor in AI ethics governance is what Fig. 3. calls “People and Planet”. This is because the people and planet can experience the negative aspects of AI in ways the designers did not imagine, and that feedback is valuable to product governance to prevent bigger AI disasters. For example, AI taking control of the air traffic control system and causing reroutes or accidents, or AI malware spreading faster than antivirus products can defend it creating a cyber pandemic. Thus, making sure bias is reduced and safety increased (DOD five AI principles) is key but certainly not easy or clear.

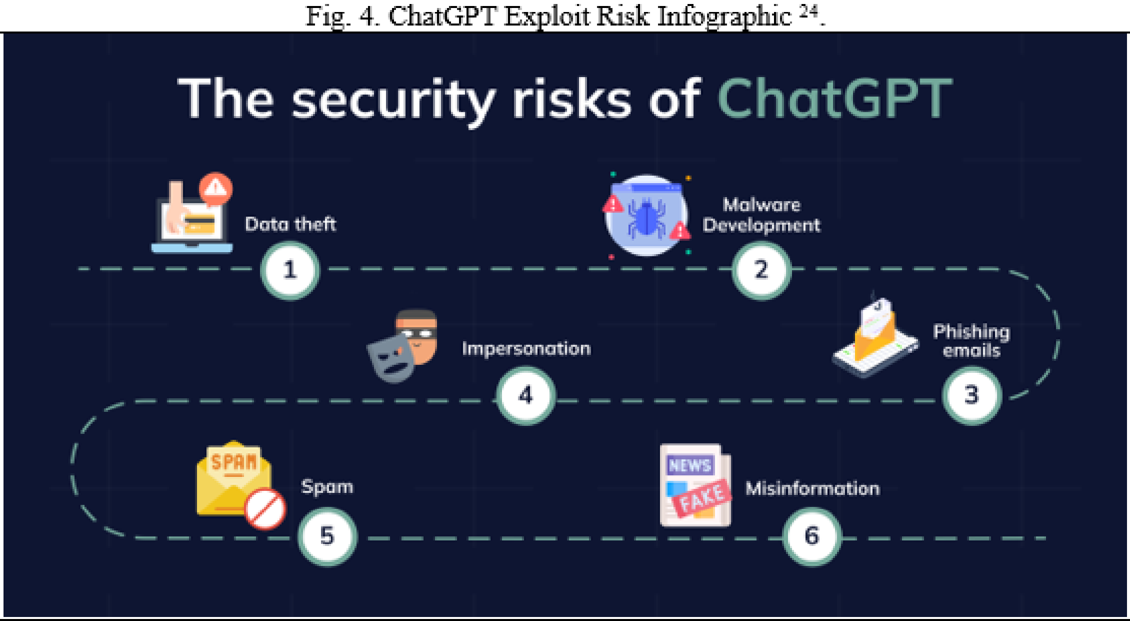
2. ChatGPT and Other Artificial Intelligence (AI) Tools Have Huge Security Risks:

It is fair to start off discussing the risks posed by ChatGPT and related tools to balance out all the positive feature coverage in the media and popular culture in recent months. First of all, with artificial intelligence (AI), every cyber threat actor has a new tool to better send spam, steal data, spread malware, build misinformation mills, grow botnets, launder cryptocurrency through shady exchanges [20], create fake profiles on multiple platforms, create fake romance chatbots, and to build the most complex self-replicating malware that will be akin to zero-day exploits much of the time.

One commentator described it this way in his well circulated LinkedIn article, “It can potentially be a formidable social engineering and phishing weapon where non-native speakers can create flawlessly written phishing emails. Also, it will be much simpler for all scammers to mimic their intended victim's tone, word choice, and writing style, making it more difficult than ever for recipients to tell the difference between a genuine and fraudulent email” [21]. Think of MailChimp on steroids with a sophisticated AI team crafting millions and billions of phishing e-mails / texts customized to impressively realistic details including phone calls with fake voices that mimic your loved ones building fake corroboration [22].

SAP’s Head of Cybersecurity Market Strategy, Gabriele Fiata, took the words out of our mouths when he described it this way, “The threat landscape surrounding artificial intelligence (AI) is expanding at an alarming rate. Between January to February 2023, Darktrace researchers have observed a 135% increase in “novel social engineering” attacks, corresponding with the widespread adoption of ChatGPT” [23]. This is just the beginning. More malware as a service propagation, fake bank sites, travel scams, and fake IT support centers will multiply to scam and extort the weak including, elders, schools, local government, and small businesses. Then there is the increased likelihood that antivirus and data loss prevention (DLP) tools will become less effective as AI morphs. Lastly, cyber criminals can and will use generative AI for advanced evidence tampering by creating fake content to confuse or dirty the chain of custody, lessen reliability, or outright frame the wrong actor – while the government is confused and behind the tech sector. It is truly a digital arms race.

Fig. 4. ChatGPT Exploit Risk Infographic [24].



In the next section we will discuss the possibilities of how artificial intelligence (AI) can enhance information security increasing compliance, reducing risk, enabling new features of great value, and enabling application orchestration for threat visibility.

3. Artificial Intelligence (AI) Powered Threat Detection Has Improved Analytics:

Artificial intelligence (AI) is increasingly being used to enhance threat detection capabilities. Machine learning algorithms analyze vast amounts of data to identify patterns indicative of potential security threats. This enables quicker and more accurate identification of malicious activities. Security information and event management (SIEM) systems enhanced with improved machine learning algorithms can detect anomalies in network traffic, application logs, and data flow – helping organizations identify potential security incidents faster.

There will be reduced false positives which has been a sustained issue in the past with large overconfident companies repeatedly wasting milling of dollars per year fine tuning useless data security lakes (we have seen this) that mostly produce garbage anomaly detection reports [25], [26]. Literally the kind good artificial intelligence (AI) laughs at - we are getting there. All the while, the technology vendors try to solve this via better SIEM functionality for an increased price at present. Yet we expect prices to drop really low as the automation matures.

With improved natural language processing (NLP) techniques, artificial intelligence (AI) systems can analyze unstructured data sources, such as social media feeds, photos, videos, and news articles - to assemble useful threat intelligence. This ability to process and understand textual data empowers organizations to stay informed about indicators of compromise (IOCs) and new attack tactics. Vendors that provide these services include Dark Trace, IBM, CrowdStrike, and many startups will likely join soon. This space is wide open and the biases of the past need to be forgotten if we want innovation. Young fresh minds who know web 3.0 are valuable here. Thus, in the future more companies will likely not have to buy but rather can build their own customized threat detection tools informed by advancements in AI platform technology.

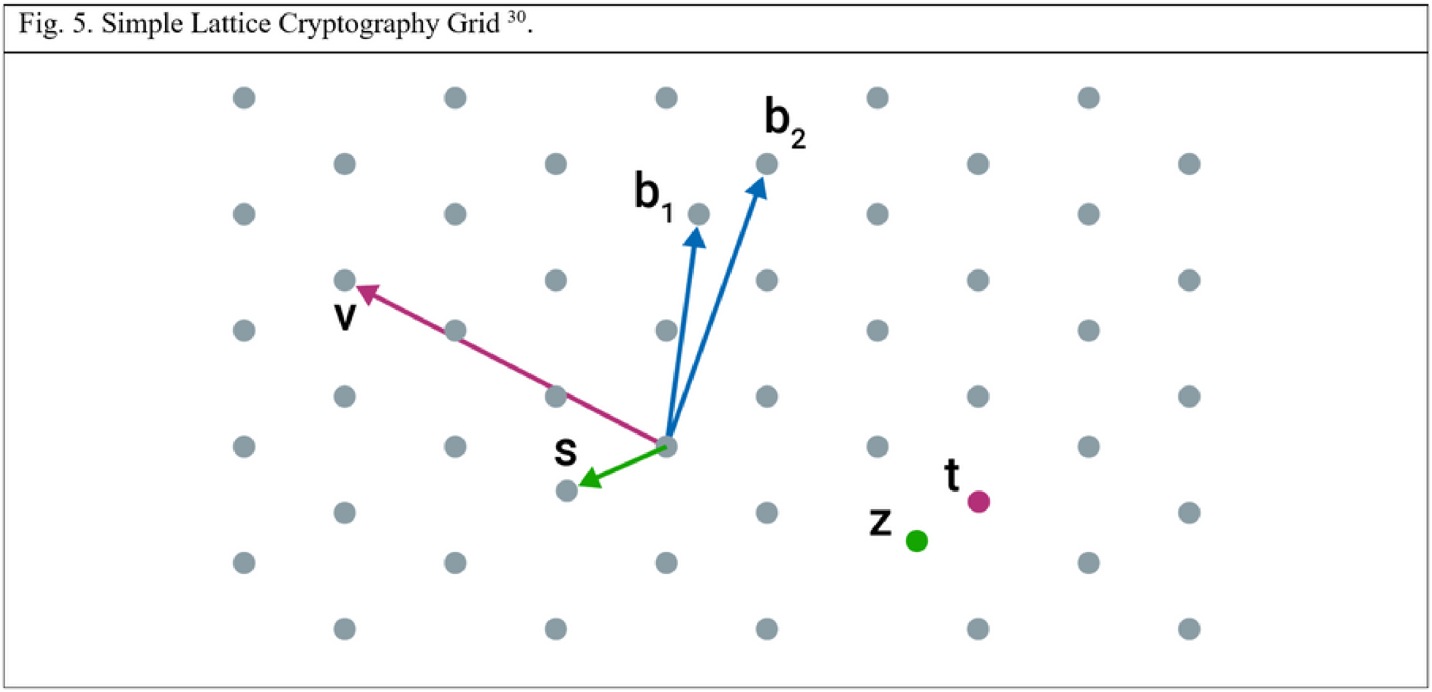
4. The Zero-Trust Security Model Becomes More Orchestrated via Artificial Intelligence (AI):

The zero-trust model assumes that no user or system, even those within the corporate network, should be trusted by default. Access controls are strictly enforced, and continuous verification is performed to ensure the legitimacy of users and devices. Zero-trust moves organizations to a need-to-know-only access mindset (least privilege) with inherent deny rules, all the while assuming you are compromised. This infers single sign-on at the personal device level and improved multifactor authentication. It also infers better role-based access controls (RBAC), firewalled networks, improved need-to-know policies, effective whitelisting and blacklisting of applications, group membership reviews, and state of the art privileged access management (PAM) tools. Password check out and vaulting tools like CyberArk will improve to better inform toxic combination monitoring and reporting. There is still work in selecting / building the right tech components that fit into (not work against) the infrastructure orchestra stack. However, we believe rapid build and deploy AI based custom middleware can alleviate security orchestration mismatches in many cases easily. All of this is likely to better automate and orchestrate zero-trust abilities so that one part does not hinder another part via complexity fog.

5. Quantum-Safe Cryptography Ripens:

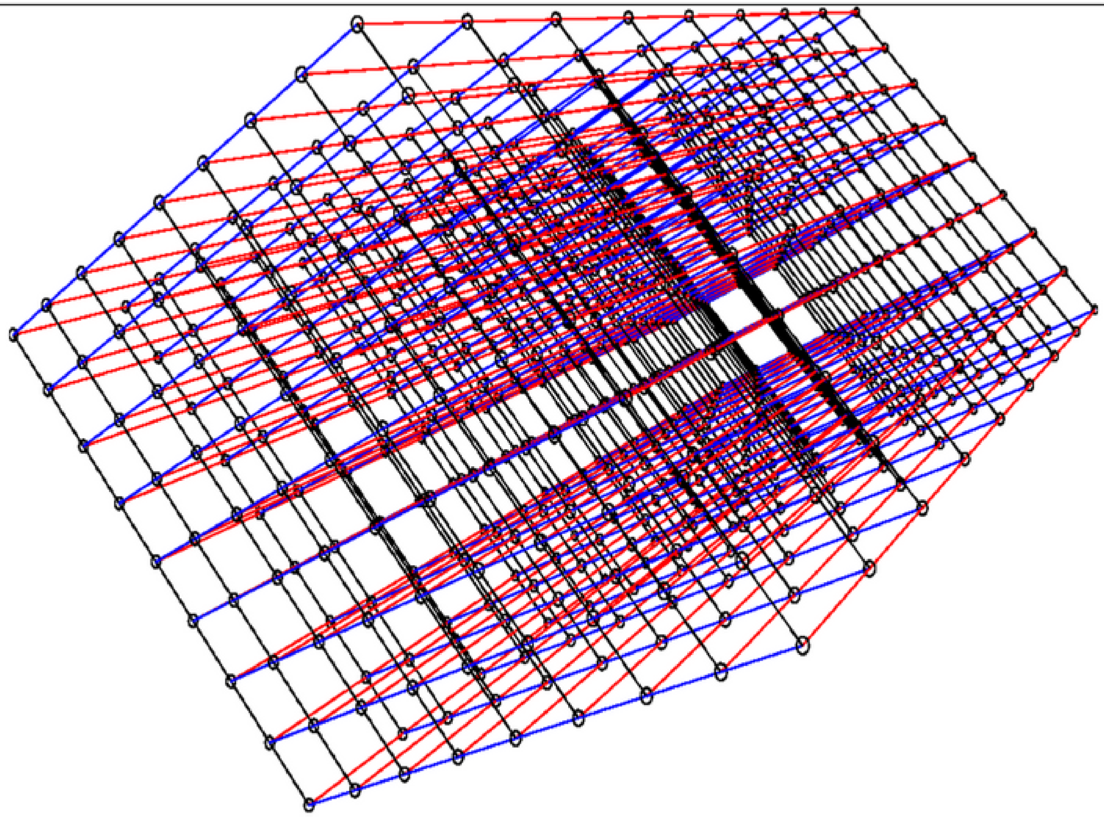
Quantum computing is a quickly evolving technology that uses the laws of quantum mechanics to solve problems too complex for traditional computers, like superposition and quantum interference [27]. Some cases where quantum computers can provide a speed boost include simulation of physical systems, machine learning (ML), optimization, and more. Traditional cryptographic algorithms could be vulnerable because they were built and coded with weaker technologies that have solvable patterns, at least in many cases. “Industry experts generally agree that within 7-10 years, a large-scale quantum computer may exist that can run Shor’s algorithm and break current public-key cryptography causing widespread vulnerabilities” [28]. Quantum-safe or quantum-resistant cryptography is designed to withstand attacks from quantum computers, often artificial intelligence (AI) assisted – ensuring the long-term security of sensitive data. For example, AI can help enhance post-quantum cryptographic algorithms such lattice-based cryptography or hash-based cryptography to secure communications [29]. Lattice-based cryptography is a cryptographic system based on the mathematical concept of a lattice. In a lattice, lines connect points to form a geometric structure or grid (Fig. 5).

Fig. 5. Simple Lattice Cryptography Grid [30].



This geometric lattice structure encodes and decodes messages. Although it looks finite, the grid is not finite in any way. Rather, it represents a pattern that continues into the infinite (Fig. 6).

Fig. 6. Complex Lattice Cryptography Grid [31].



Lattice based cryptography benefits sensitive and highly targeted assets like large data centers, utilities, banks, hospitals, and government infrastructure generally. In other words, there will likely be mass adoption of quantum computing based encryption for better security. Lastly, we used ChatGPT as an assistant to compile the below specific benefits of quantum cryptography albeit with some manual corrections [32]:

a. **Detection of Eavesdropping:**
Quantum key distribution protocols can detect the presence of an eavesdropper by the disturbance introduced during the quantum measurement process, providing a level of security beyond traditional cryptography.

b. **Quantum-Safe Against Future Computers**
Quantum computers have the potential to break many traditional cryptographic systems. Quantum cryptography is considered quantum-safe, as it relies on the fundamental principles of quantum mechanics rather than mathematical complexity.

c. **Near Unconditional Security:**
Quantum cryptography provides near unconditional security based on the principles of quantum mechanics. Any attempt to intercept or measure the quantum state will disturb the system, and this disturbance can be detected. Note that ChatGPT wrongly said “unconditional Security” and we corrected to “near unconditional security” as that is more realistic.

6. Artificial Intelligence (AI) Streamline Cloud Security Posture Management (CSPM):

As organizations increasingly migrate to cloud environments, ensuring the security of cloud assets becomes key. Vendors like Microsoft, Oracle, and Amazon Web Services (AWS) lead this space; yet large organizations have their own clouds for control as well. Cloud security posture management (CSPM) tools help organizations manage and secure their cloud infrastructure by continuously monitoring configurations and detecting misconfigurations that could lead to vulnerabilities [33]. These tools automatically assess cloud configurations for compliance with security best practices. This includes ensuring that only necessary ports are open, and that encryption is properly configured. “Keeping data safe in the cloud requires a layered defense that gives organizations clear visibility into the state of their data. This includes enabling organizations to monitor how each storage bucket is configured across all their storage services to ensure their data is not inadvertently exposed to unauthorized applications or users” [34]. This has considerations at both the cloud user and provider level especially considering artificial intelligence (AI) applications can be built and run inside the cloud for a variety of reasons. Importantly, these build designs often use approved plug ins from different vendors making it all the more complex.

7. Artificial Intelligence (AI) Driven Threat Response Ability Advances:

Artificial intelligence (AI) is used not only for threat detection but also in automating response actions [35]. This can include automatically isolating compromised systems, blocking malicious internet protocol (IP) addresses, closing firewalls, or orchestrating a coordinated response to a cyber incident – all for less money. Security orchestration, automation, and response (SOAR) platforms leverage AI to analyze and respond to security incidents, allowing security teams to automate routine tasks and respond more rapidly to emerging threats. Microsoft Sentinel, Rapid7 InsightConnect, and FortiSOAR are just a few of the current examples. Basically, AI tools will help SOAR tools mature so security operations centers (SOCs) can catch the low hanging fruit; thus, they will have more time for analysis of more complex threats. These AI tools will employ the observe, orient, decide, act (OODA) Loop methodology [36]. This will allow them to stay up to date, customized, and informed of many zero-day exploits. At the same time, threat actors will constantly try to avert this with the same AI but with no governance.

8. Artificial Intelligence (AI) Enhanced Authentication Arrives:

Artificial intelligence (AI) is being utilized to strengthen user authentication methods. Behavioral biometrics, such as analyzing typing patterns, mouse movements and ram usage, can add an extra layer of security by recognizing the unique behavior of legitimate users. Systems that use AI to analyze user behavior can detect and flag suspicious activity, such as an unauthorized user attempting to access an account or escalate a privilege [37]. Two factor authentication remains the bare standard with many leading identity and access management (IAM) application makers including Okta, SailPoint, and Google experimenting with AI for improved analytics and functionality. Both two factor and multifactor authentication benefit from AI advancements with machine learning via real time access rights reassignment and improved role groupings [38]. However, multifactor remains stronger at this point because it includes something you are, biometrics. The jury is out on which method will remain the security leader because biometrics can be faked by AI [39]. Importantly, AI tools can remove fake accounts or orphaned accounts much more quickly, reducing risk. However, it likely will not get it right 100% of the time so there is a slight inconvenience.

Conclusion and Recommendations:

Artificial intelligence (AI) remains a leading catalyst for digital transformation in tech automation, identity and access management (IAM), big data analytics, technology orchestration, and collaboration tools. AI based quantum computing serves to bolster encryption when old methods are replaced. All of the government actions to incubate ethics in AI are a good start and the NIST AI Risk Management Framework (AI RMF) 1.0 is long overdue. It will likely be tweaked based on private sector feedback. However, adding the DOD five principles for the ethical development of AI to the NIST AI RMF could derive better synergies. This approach should be used by the private sector and academia in customized ways. AI product ethical deviations should be thought of as quality control and compliance issues and remediated immediately.

Organizations should consider forming an AI governance committee to make sure this unique risk is not overlooked or overly merged with traditional web / IT risk. ChatGPT is a good encyclopedia and a cool Boolean search tool, yet it got some things wrong about quantum computing in this article for which we cited and corrected. The Simplified AI text to graphics generator was cool and useful but it needed some manual edits as well. Both of these generative AI tools will likely get better with time.

Artificial intelligence (AI) will spur many mobile malware and ransomware variants faster than Apple and Google can block them. This in conjunction with the fact that people more often have no mobile antivirus on their smart phone even if they have it on their personal and work computers, and a culture of happy go lucky application downloading makes it all the worse. As a result, more breaches should be expected via smart phones / watches / eyeglasses from AI enabled threats.

Therefore, education and awareness around the review and removal of non-essential mobile applications is a top priority. Especially for mobile devices used separately or jointly for work purposes. Containerization is required via a mobile device management (MDM) tool such as JAMF, Hexnode, VMWare, or Citrix Endpoint Management. A bring your own device (BYOD) policy needs to be written, followed, and updated often informed by need-to-know and role-based access (RBAC) principles. This requires a better understanding of geolocation, QR code scanning, couponing, digital signage, in-text ads, micropayments, Bluetooth, geofencing, e-readers, HTML5, etc. Organizations should consider forming a mobile ecosystem security committee to make sure this unique risk is not overlooked or overly merged with traditional web / IT risk. Mapping the mobile ecosystem components in detail is a must including the AI touch points.

The growth and acceptability of mass work from home (WFH) combined with the mass resignation / gig economy remind employers that great pay and culture alone are not enough to keep top talent. At this point, AI only takes away some simple jobs but creates AI support jobs, yet the percents of this are not clear this early. Signing bonuses and personalized treatment are likely needed for those with top talent. We no longer have the same office and thus less badge access is needed. Single sign-on (SSO) will likely expand to personal devices (BYOD) and smart phones / watches / eyeglasses. Geolocation-based authentication is here to stay with double biometrics, likely fingerprint, eye scan, typing patterns, and facial recognition. The security perimeter remains more defined by data analytics than physical / digital boundaries, and we should dashboard this with machine learning tools as the use cases evolve.

Cloud infrastructure will continue to grow fast creating perimeter and compliance complexity / fog. Organizations should preconfigure artificial intelligence (AI) based cloud-scale options and spend more on cloud-trained staff. They should also make sure that they are selecting more than two or three cloud providers, all separate from one another. This helps staff get crosstrained on different cloud platforms and plug in applications. It also mitigates risk and makes vendors bid more competitively. There is huge potential for AI synergies with Cloud Security Posture Management (CSPM) tools, and threat response tools - experimentation will likely yield future dividends. Organization should not be passive and stuck in old paradigms. The older generations should seek to learn from the younger generations without bias. Also, comprehensive logging is a must for AI tools.

In regard to cryptocurrency, non-fungible tokens (NFTs), initial coin offerings (ICOs), and related exchanges – artificial intelligence (AI) will be used by crypto scammers and those seeking to launder money. Watch out for scammers who make big claims without details, no white papers or filings, or explanations at all. No matter what the investment, find out how it works and ask questions about where your money is going. Honest investment managers and advisors want to share that information and will back it up with details in many documents and filings [40]. Moreover, better blacklisting by crypto exchanges and banks is needed to stop these illicit transactions erroring far on the side of compliance. This requires us to pay more attention to knowing and monitoring our own social media baselines – emerging AI data analytics can help here. If you are for and use crypto mixer and / or splitter services then you run the risk of having your digital assets mixed with dirty digital assets, you have high fees, you have zero customer service, no regulatory protection, no decent Terms of Service and / or Privacy Policy if any, and you have no guarantee that it will even work the way you think it will.

As security professionals, we are patriots and defenders of wherever we live and work. We need to know what our social media baseline is across platforms. IT and security professionals need to realize that alleviating disinformation is about security before politics. We should not be afraid to talk about this because if we are, then our organizations will stay weak and outdated and we will be plied by the same artificial intelligence (AI) generated political bias that we fear confronting. More social media training is needed as many security professionals still think it is mostly an external marketing thing.

It's best to assume AI tools are reading all social media posts and all other available articles, including this article which we entered into ChatGPT for feedback. It was slightly helpful pointing out other considerations. Public-to-private partnerships (InfraGard) need to improve and application to application permissions need to be more scrutinized. Everyone does not need to be a journalist, but everyone can have the common sense to identify AI / malware-inspired fake news. We must report undue AI bias in big tech from an IT, compliance, media, and a security perspective. We must also resist the temptation to jump on the AI hype bandwagon but rather should evaluate each tool and use case based on the real-world business outcomes for the foreseeable future.

About the Authors:

Jeremy Swenson is a disruptive-thinking security entrepreneur, futurist / researcher, and senior management tech risk consultant. He is a frequent speaker, published writer, podcaster, and even does some pro bono consulting in these areas. He holds an MBA from St. Mary's University of MN, an MSST (Master of Science in Security Technologies) degree from the University of Minnesota, and a BA in political science from the University of Wisconsin Eau Claire. He is an alum of the Federal Reserve Secure Payment Task Force, the Crystal, Robbinsdale and New Hope Citizens Police Academy, and the Minneapolis FBI Citizens Academy.

Matthew Versaggi is a senior leader in artificial intelligence with large company healthcare experience who has seen hundreds of use-cases. He is a distinguished engineer, built an organization's "College of Artificial Intelligence", introduced and matured both cognitive AI technology and quantum computing, has been awarded multiple patents, is an experienced public speaker, entrepreneur, strategist and mentor, and has international business experience. He has an MBA in international business and economics and a MS in artificial intelligence from DePaul University, has a BS in finance and MIS and a BA in computer science from Alfred University. Lastly, he has nearly a dozen professional certificates in AI that are split between the AI, technology, and business strategy.

References:

[1] Swenson, Jeremy, and NIST; Mashup 12/15/2023; "Artificial Intelligence Risk Management Framework (AI RMF 1.0)". 01/26/23: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.
[2] Swenson, Jeremy, and Simplified AI; AI Text to graphics generator. 01/08/24: https://app.simplified.com/
[3] Swenson, Jeremy, and ChatGPT; ChatGPT Logo Mashup. OpenAI. 12/15/23: https://chat.openai.com/auth/login
[4] The White House; "Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." 10/30/23: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/
[5] Nerdynav; "107 Up-to-Date ChatGPT Statistics & User Numbers [Dec 2023]." 12/06/23: https://nerdynav.com/chatgpt-statistics/
[6] Sun, Zhiyuan; "Two individuals indicted for $25M AI crypto trading scam: DOJ." Cointelegraph. 12/12/23: https://cointelegraph.com/news/two-individuals-indicted-25m-ai-artificial-intelligence-crypto-trading-scam
[7] Nerdynav; "107 Up-to-Date ChatGPT Statistics & User Numbers [Dec 2023]." 12/06/23: https://nerdynav.com/chatgpt-statistics/
[8] Nerdynav; "107 Up-to-Date ChatGPT Statistics & User Numbers [Dec 2023]." 12/06/23: https://nerdynav.com/chatgpt-statistics/
[9] The White House; "Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." 10/30/23: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/
[10] EU. "EU AI Act: first regulation on artificial intelligence." 12/19/23: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
[11] Jackson, Amber; "Top 10 companies with ethical AI practices." AI Magazine. 07/12/23: https://aimagazine.com/ai-strategy/top-10-companies-with-ethical-ai-practices
[12] Golbin, Ilana, and Axente, Maria Luciana; "9 ethical AI principles for organizations to follow." World Economic Forum and PricewaterhouseCoopers (PWC). 06/23/21 https://www.weforum.org/agenda/2021/06/ethical-principles-for-ai/
[13] Lopez, Todd C; "DOD Adopts 5 Principles of Artificial Intelligence Ethics". DOD News. 02/25/20: https://www.defense.gov/News/News-Stories/article/article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/
[14] Golbin, Ilana, and Axente, Maria Luciana; "9 ethical AI principles for organizations to follow." World Economic Forum and PricewaterhouseCoopers (PWC). 06/23/21 https://www.weforum.org/agenda/2021/06/ethical-principles-for-ai/
[15] The Office of the Director of National Intelligence. "Principles of Artificial Intelligence Ethics for the Intelligence Community." 07/23/20: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2020/3468-intelligence-community-releases-artificial-intelligence-principles-and-framework#:~:text=The%20Principles%20of%20AI%20Ethics,resilient%20by%20design%2C%20and%20incorporate
[16] NIST; "NIST AI RMF Playbook." 01/26/23: https://airc.nist.gov/AI_RMF_Knowledge_Base/Playbook

[17] NIST; “Artificial Intelligence Risk Management Framework (AI RMF 1.0).” 01/26/23: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
[18] NIST; “Artificial Intelligence Risk Management Framework (AI RMF 1.0).” 01/26/23: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
[19] Crafts, Nicholas; “Artificial intelligence as a general-purpose technology: an historical perspective.” Oxford Review of Economic Policy. Volume 37, Issue 3, Autumn 2021: https://academic.oup.com/oxrep/article/37/3/521/6374675
[20] Sun, Zhiyuan; “Two individuals indicted for $25M AI crypto trading scam: DOJ.” Cointelegraph. 12/12/23: https://cointelegraph.com/news/two-individuals-indicted-25m-ai-artificial-intelligence-crypto-trading-scam
[21] Patel, Pranav; “ChatGPT brings forth new opportunities and challenges to the Cybersecurity industry.” LinkedIn Pulse. 04/03/23: https://www.linkedin.com/pulse/chatgpt-brings-forth-new-opportunities-challenges-industry-patel/
[22] FTC; “Preventing the Harms of AI-enabled Voice Cloning.” 11/16/23: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/preventing-harms-ai-enabled-voice-cloning
[23] Fiata, Gabriele; “Why Evolving AI Threats Need AI-Powered Cybersecurity.” Forbes. 10/04/23: https://www.forbes.com/sites/sap/2023/10/04/why-evolving-ai-threats-need-ai-powered-cybersecurity/?sh=161bd78b72ed
[24] Patel, Pranav; “ChatGPT brings forth new opportunities and challenges to the Cybersecurity industry.” LinkedIn Pulse. 04/03/23: https://www.linkedin.com/pulse/chatgpt-brings-forth-new-opportunities-challenges-industry-patel/
[25] Tobin, Donal; “What Challenges Are Hindering the Success of Your Data Lake Initiative?” Integrate.io. 10/05/22: https://www.integrate.io/blog/data-lake-initiative/
[26] Chuvakin, Anton; “Why Your Security Data Lake Project Will … Well, Actually …” Medium. 10/22/22. https://medium.com/anton-on-security/why-your-security-data-lake-project-will-well-actually-78e0e360c292
[27] Amazon Web Services; “What are the types of quantum technology?” 01/07/23: https://aws.amazon.com/what-is/quantum-computing/
[28] ISARA Corporation; “What is Quantum-safe Cryptography?” 2023: https://www.isara.com/resources/what-is-quantum-safe.html
[29] Swenson, Jeremy, and ChatGPT; OpenAI. 12/15/23: https://chat.openai.com/auth/login
[30] Utimaco; “What is Lattice-based Cryptography? 2023: https://utimaco.com/service/knowledge-base/post-quantum-cryptography/what-lattice-based-cryptography
[31] D. Bernstein, and T. Lange; “Post-quantum cryptography - dealing with the fallout of physics success.” IACR Cryptology. 2017: https://www.semanticscholar.org/paper/Post-quantum-cryptography-dealing-with-the-fallout-Bernstein-Lange/a515aad9132a52b12a46f9a9e7ca2b02951c5b82
[32] Swenson, Jeremy, and ChatGPT; OpenAI. 12/15/23: https://chat.openai.com/auth/login
[33] Microsoft; “What is CSPM?” 01/07/24: https://www.microsoft.com/en-us/security/business/security-101/what-is-cspm
[34] Rosencrance, Linda; “How to choose the best cloud security posture management tools.” CSO Online. 10/30/23: https://www.csoonline.com/article/657138/how-to-choose-the-best-cloud-security-posture-management-tools.html

[35] Sibanda, Isla; “AI and Machine Learning: The Double-Edged Sword in Cybersecurity.” RSA Conference. 12/13/23: https://www.rsaconference.com/library/blog/ai-and-machine-learning-the-double-edged-sword-in-cybersecurity
[36] Michael, Katina, Abbas, Roba, and Roussos, George; “AI in Cybersecurity: The Paradox.” IEEE Transactions on Technology and Society. Vol. 4, no. 2: pg. 104-109. 2023: https://ieeexplore.ieee.org/abstract/document/10153442
[37] Muneer, Salman Muneer, Muhammad Bux Alvi, and Amina Farrakh; “Cyber Security Event Detection Using Machine Learning Technique.” International Journal of Computational and Innovative Sciences. Vol. 2, no (2): pg. 42-46. 2023: https://ijcis.com/index.php/IJCIS/article/view/65.
[38] Azhar, Ishaq; “Identity Management Capability Powered by Artificial Intelligence to Transform the Way User Access Privileges Are Managed, Monitored and Controlled.” International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Vol. 9, Issue 1: pg. 4719-4723. January 2021: https://ssrn.com/abstract=3905119
[39] FTC; “Preventing the Harms of AI-enabled Voice Cloning.” 11/16/23: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/preventing-harms-ai-enabled-voice-cloning
[40] FTC; “What To Know About Cryptocurrency and Scams.” May 2022: https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams

The Python Programming Language Numerical Analysis/Machine Learning Series

By Constantinos Dokas
ISSA member, North Virginia (NOVA) Chapter

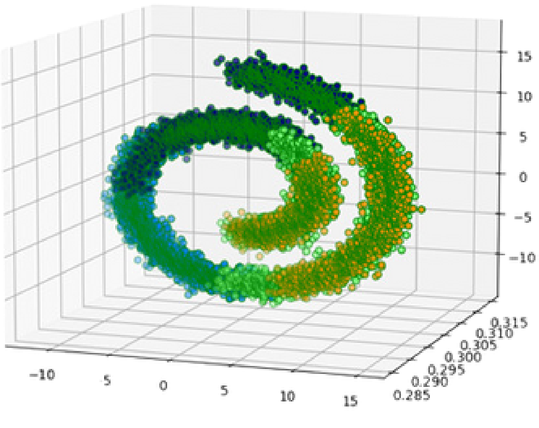
This article is part of a series of articles which deals with topics in programming using the Python programming language. In previous articles we presented Python programs which use linear regression, multi-linear regression, supervised learning algorithm, logistic regression, decision tree, random forest, ensemble voting, and GBRT/XGBOOST algorithms.

In this article we will continue with a discussion of the dimensionality issue and its solutions. We will also continue development of the program which acquires IP info from online databases.

DIMENSIONALITY ISSUES

So far we have worked with datasets that have very few features. However, ML problems have huge amounts of features and make processing of them slow, and leading to inaccurate predictions. Data scientists often refer to that issue as the curse of dimensionality. Therefore, methods to reduce the number of features were studied and tested. Each type of data that we process needs to be handled carefully because eliminating features is information loss and may lead to errors. Having said that, we need to study the features and eliminate those who either have no effect or their effect is minimal. Methods of dimensionality reduction do exist and we will briefly discuss them in this article.

Fig1. Swiss Roll Example



One concept that is often used in reducing the dimensions of a dataset is related to study of Swiss roll datasets.

This method is called *manifold learning* and is based on the *manifold hypothesis* or *manifold assumption.* The hypothesis suggests that high dimensional datasets are close to a manifold of lower dimensions. Another concept is called *projection.* This concept is based on the fact that many times the training instances are not spread equally in all the dimensions. In that case all we need to do is to identify the group of data which lie within a lower amount of dimensions. Then, we project the outliers of that group into the group's subspace. In this way we get the final group of instances which will be used to train our program.

The most popular dimensionality reduction algorithm is the PCA or *Principal Component Analysis*. The focal point of this algorithm is to find the proper hyperplane on which data must be projected. Developed by Karl Pearson in 1901, it was adapted throughout the years by other scientists in a number of disciplines like signal processing, mechanical engineering, and meteorological science, to mention a few. It is a fascinating topic to study.

Another algorithm the *Locally Linear Embedding* or LLE is using the *Manifold Learning* method instead of projections. The algorithm identifies the closest neighbors of each instance and reconstructs that instance as a linear function of these neighbors. The end result is the unrolling of the Swiss roll while the distances between those instances are not altered. This algorithm performs well on small and medium size datasets.

Isomap, *Isometric Mapping*, is another algorithm. This also works with neighbors of each instance but it is attempting to preserve the *geodesic distance* between instances during the reduction Note that the shortest path, an arc length, between two points on a curved surface is called the *geodesic distance*.

Another algorithm, t-SNE is mostly used for visualization projects. Also LDA, Linear Discriminant Analysis, is an algorithm that is used to reduce dimensionality. It is utilized as preprocessor before another algorithm which does the final processing of the data.

IP INFO PROJECT

We will continue building up on the project which we started in January.

The task is as follows:
You have received, from a department in your company, a text file that contains IP data. The file contains one IP per line. You do not know how the file was created or if all the data is valid. You should look in the web and find which country and entity owns the data. You are tasked to isolate the valid data and develop some statistics related to it. You must return the data back to the sender in a database format.

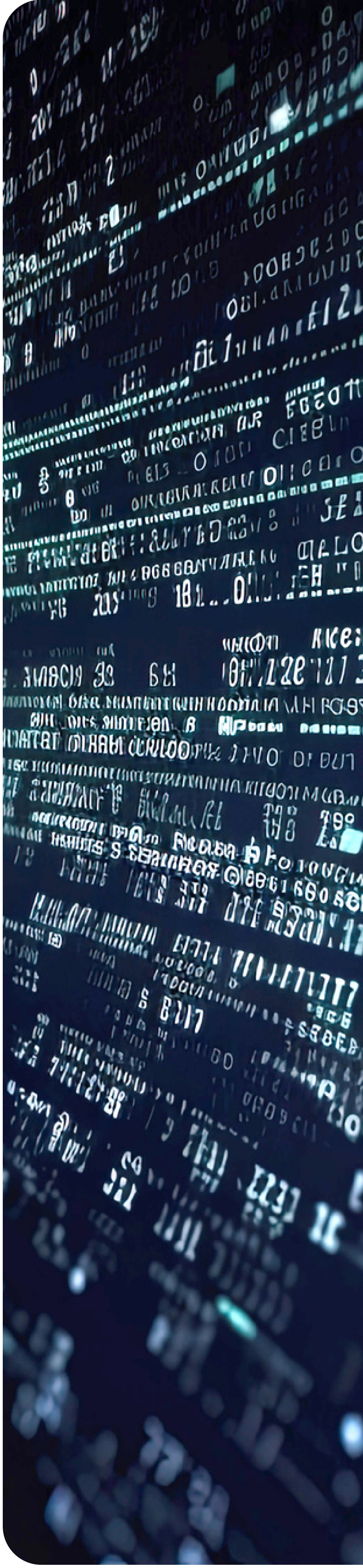
You have decided to have the program create the following outputs:
1) Listing of the data on Python's shell for a quick examination.
2) Create a log that contains all the errors that were encountered.
3) Create an SQlite database with the following information ip, description, country, date.
4) Create some SQL statements to pull data and statistics from the database.

For better handling of the data you have decided to create two Python programs to complete the task. The first program will process and organize the data. This program will isolate good data, report errors, log errors in a text log file, and create the database that contains clean data organized as requested. The second program is to test the database and create some statistics.

First program

CODE

```
from ipwhois import IPWhois
import sqlite3
from sqlite3 import Error

def create_and_load_db(dbname):
  dbconn = None # -- database connect string
  try:
    dbconn = sqlite3.connect(dbname)
  except Error as e:
    print("Unable to create database", dbname, "\n\t\t\t",e)
  finally:
    if dbconn:
      # ---
      dbcursor = dbconn.cursor()
      # ---
      dbcursor.execute('DROP TABLE IF EXISTS ipmaininfo')
      # --
      main_table_sql = '''CREATE TABLE IF NOT EXISTS ipmaininfo(
                    ip text PRIMARY KEY,
                    description text NOT NULL,
                    country text NOT NULL,
                    date text NOT NULL
                    );'''
      create_table(dbcursor, main_table_sql)
      # ---
      main_table_insert_sql = “‘INSERT INTO
                        ipmainininfo(ip,description,country,date) VALUES(“‘
      load_table(dbcursor, main_table_insert_sql, IP_data)
      dbconn.commit()
      dbconn.close()

def create_table(dbcursor, tblsql):

  dbcursor.execute(tblsql)
  return dbcursor

def load_table(dbcursor, insertsql, data):
  for ip_key in data.keys():
    new_insert_sql = insertsql+'"'+ip_key+'"'+','+data[ip_key]+');'
    dbcursor.execute(new_insert_sql)

keys=['asn_description','asn_country_code', 'asn_date']
# --- Function
def parseIPinfo(ip_dictionary,keys):
  ip_info=""          # -- Empty string
  for a_key in keys:
    print(a_key,ip_dictionary[a_key])
    ip_info=ip_info+'"'+ip_dictionary[a_key].replace(',','')+'",'
  ip_info=ip_info[:len(ip_info)-1]
  print("---")
  return ip_info

# --- End of Function

# --- Program execution starts here ----------------------
ListofIPs=[]
IP_networkData=[]
ErrorLog={}
BlankLines=0
IP_data={}

with open("IP_List.txt",mode='r') as myIPfile:
  for ip in myIPfile:
    print('\n',ip,end='')
    ip=ip.strip()
    ListofIPs.append([ip])
    if len(ip) < 1:
      BlankLines+=1
      continue
    try:
```



```
       IPwhoInf=IPWhois(ip)
      myLookupDictionary = None
      myLookupDictionary = IPwhoInf.lookup_whois()
      for key in myLookupDictionary.keys():
        if 'nets' in key:
          if len(myLookupDictionary[key]) > 1:
            print("===> ",key," multiples ", len(myLookupDictionary[key]))
      info = parseIPinfo(myLookupDictionary,keys)
      IP_data[ip]=info
      print(IP_data)
    except BaseException as serr:
      ErrorLog[ip]=f"Unexpected {err=}, {type(err)=}"

#----------------------- Display on IDLE Shell ------
print("Blank lines encountered",BlankLines)
if len(ErrorLog) > 0:
  print("\nErrors",len(ErrorLog),"\n---------")
  for key in ErrorLog.keys():
    print(ErrorLog[key],"\n")
#----------------------- Store in a File ------------
with open("ErrorLog.txt",mode='w') as myErrorLog:
  if len(ErrorLog) > 0:
    for key in ErrorLog.keys():
      myErrorLog.write(ErrorLog[key]+'\n\n')
#----------------------- Store in a Database ---------
create_and_load_db('ip_info_db.db')
```

OUTPUT

The output of the program on Python's shell is as follows (same as in previous article with some additions):

```
 205.180.54.9
asn_description LEVEL3, US
asn_country_code US
asn_date 1995-03-21
---
...
Errors 6
---------
Unexpected err=IPDefinedError('IPv4 address 233.109.54.21 is already defined as Multicast via
RFC 3171.'), type(err)=<class 'ipwhois.exceptions.IPDefinedError'>
...
```

The data in the log file is:

```
Unexpected err=IPDefinedError('IPv4 address 233.109.54.21 is already defined as Multicast via RFC 3171.'), type(err)=<class 'ipwhois.exceptions.IPDefinedError'>

Unexpected err=IPDefinedError('IPv4 address 233.161.54.50 is already defined as Multicast via RFC 3171.'), type(err)=<class 'ipwhois.exceptions.IPDefinedError'>

Unexpected err=ValueError("'322.61.54.71' does not appear to be an IPv4 or IPv6 address"), type(err)=<class 'ValueError'>
...
```

DISCUSSION

The first program was developed without a *main()* function. When you create quick scripts you can omit that function. We will use *main()* in the second program.

Note that we are using a *try/except* construct to catch any errors that may be created during the opening of the database. You may add this type of construct to other parts of your program. However, keep in mind that these blocks will slow the execution of the code.

When inserting values in text table fields make sure that there are no embedded commas in the values. A comma (,) will be interpreted as field separator and you will get an error. To remove them use *valuename*.**replace**(',',''). Also, do not forger to convert to strings numeric type of data or data that contains special characters.

In this program we created the IP database field as primary key. Therefore, we assumed that there are no duplicates in our source. If you are not sure then you have a choice to:
a) Do not make the field a primary key
b) Develop logic to handle the resulting error and either skip it or update the data stored on that record.

Second program

CODE

```
import sqlite3
from sqlite3 import Error
import os
# --
def open_db(dbname):
  dbconn = None # database connect string
  try:
        dbconn = sqlite3.connect(dbname)
    except Error as e:
        print("Unable to create database", dbname, "\n\t\t\t",e)
    finally:
        return dbconn
# --
def list_by_country(dbconn):
    # -- SELECT statement
    select_statement='''SELECT country, ip FROM ipmaininfo ORDER BY country'''
    cursor = dbconn.cursor()
    cursor.execute(select_statement)
    rows = cursor.fetchall()

    for row in rows:
        print(row)
# --
def country_totals(dbconn):
    select_statement=”‘SELECT country, COUNT(*) FROM ipmaininfo GROUP BY country“‘

    cursor = dbconn.cursor()
    cursor.execute(select_statement)
    rows = cursor.fetchall()
    for row in rows:
        print(row)
# --                    ----
def main():
    databaseName = 'ip_info_db.db'
    if os.path.isfile(databaseName) == True:
        dbconn = open_db(databaseName )
        if dbconn:
            print('connected to database')
            list_by_country(dbconn)
            country_totals(dbconn)
            dbconn.close()
    else:
        print("file",databaseName,"was not found!")
# -- Processing starts here
if __name__ == '__main__':
    main()
```

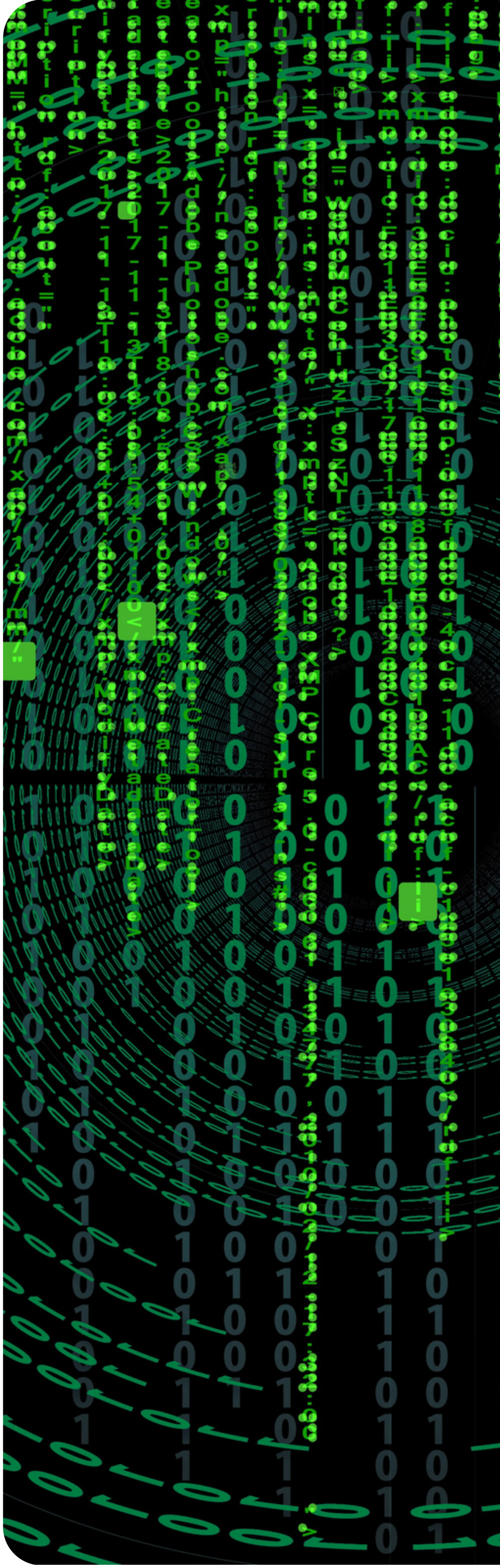
OUTPUT

Country and IP listing

```
connected to database
('AU', '203.173.42.38')
('BR', '200.160.35.20')
('BR', '200.169.41.28')
('CA', '205.189.54.15')
('CN', '222.189.54.15')
('CN', '222.61.54.71')
('CN', '219.129.34.7')
('CN', '218.200.89.11')
('CN', '218.200.211.12')
('FI', '213.161.54.71')
('JP', '210.189.54.15')
('JP', '210.161.54.71')
('JP', '211.120.34.7')
('JP', '218.129.37.34')
('MX', '201.136.5.9')
('MX', '201.161.54.71')
('SG', '202.161.54.71')
('SG', '202.167.12.41')
('US', '205.180.54.9')
('US', '205.180.59.11')
('US', '205.161.54.71')
('US', '214.161.54.71')
```

Occurrences per country

```
('AU', 1)
('BR', 2)
('CA', 1)
('CN', 5)
('FI', 1)
('JP', 4)
('MX', 2)
('SG', 2)
('US', 4)
```



DISCUSSION

The database processing program is using code similar to code used in articles a couple years ago (Titanic ship data processing and analysis).

Note that the program was organized in a format which we use in developing commercial software. It consists of three major blocks; module import block, function definition block, main process block.

The first task for the program to complete is to ensure that the database file does exist in the same directory with the program code. For this the **os** python module is used. From that module the **path** *object* and its **isfile** *method* are used to determine if the database file is available. Then processing continues, if the database file is available and if the program can successfully connect to it. Therefore, if there were no errors the program proceeds with calling the two functions which were previously defined; *list_by_country(), country_totals()*.

Next the program opens the database and creates a list of the IP and country columns. The data is sorted by country. The next task is to provide a count of IPs for each country that is represented in the data. To accomplish this the data is first grouped by country and then the counts are created.

WHAT IS IN THE NEXT ARTICLE

In the next article we will continue on ML algorithms and also update the IP info program which was started in the previous article. Keep all of these articles in your library because the code in each article assumes that you are already familiar with concepts previously posted. Please note that my email (cdoskas@megabizhost.com) is available for your comments. Use this email address if you have any questions related to specific topics of this article.

CONCLUSION

To conclude, this article presented an overview of the ML issue which is related for the existence of too many features in a dataset. In addition, the programming task of creating IP related information and statistics was furthermore developed.
I encourage you to study the concepts presented in this and previous articles and find ways to improve or add to the presented code. See you again through the next article.

NEWS FROM THE FOUNDATION

Announcing the top three leaders in the **ISSA Chapter Challenge Contest (CCC)** through the end of 2023:

- **$1,020 Denver**
- **$ 750 Charlotte Metro**
- **$ 500 Northern Colorado**

Ask your Chapter Leaders how your Chapter can participate in the contest by holding a fundraising event to benefit the Foundation's scholarship fund.

Get in the race - up your donation to become #1. If your Chapter is competing for one of the ISSA Chapter of the Year awards, a donation would be a good addition to your application. Let the world know you're out there - Go for it! More information can be found in the **CCC Guide** on the ISSAEF website. Contest is open until the end of June.

To donate for your chapter, visit:
www.issaef.org/donate/CCC

BECOME A VOLUNTEER!

The Foundation is seeking individuals to fill the following volunteer positions:

- **Financial Auditor** to audit Foundation books. This is a one-time project. A CPA license is *not* required.
- **Director of Communications.** Write articles about our activities for the ISSA Journal and create posts on our social media pages, i.e. LinkedIn, Facebook, etc.
- **Scholarship Review Committee** members needed to evaluate applications for the 2024 review cycle.

CPE's are given for each of these positions. Interested? Email us at: Volunteer@issaef.org to learn more.

The **2024 Scholarship & Grants Application** period opened to receive applications on February 1st. Scholarship applicants have until **June 15th** to submit their applications with required accompanying documentation. Grant applications are accepted until **April 30th.** Remember that even if you've applied before (awardee or not) you can apply every year that you meet the qualifications.
Visit our website to learn more:
www.issaef.org/scholarships/

The **Cloud Security Alliance** (CSA) grant for 2024 was erroneously stated in the January ISSA Journal as being for $2,200, however the correct amount is $2,000 total. This grant gives amounts (ranging between $250 to $1,000) for individuals seeking to increase their knowledge and understanding of cybersecurity

The Cyber Executive Forum is a peer-to-peer event - Members can feel free to share concerns, successes, and feedback in a peer-only environment.

ISSA CYBER EXECUTIVE MEMBERSHIP PROGRAM

The role of information security executive continues to be defined and redefined as the integration of business and technology as it evolves. While these new positions gain more authority and responsibility, peers must form a collaborative environment to foster knowledge and influence that will shape the profession.

The Information Systems Security Association (ISSA) recognizes this need and created the exclusive Cyber Executive Membership program to give executives an environment to achieve mutual success. Connecting professionals to a large network or peers, valuable information, and top industry experts the program is a functional resource for members to advance personal and industry understanding of critical issues in information security

MEMBERSHIP BENEFITS

- Free registration at four Cyber Executive Forums per year, including lodging for one night and all meals at each Forum
- You'll be part of an effective forum for understanding and influencing relevant standards and legislation
- Extensive networking opportunities with peers and experts on an ongoing basis
- Direct access to top subject matter experts through educational seminars
- CPE credits you earn will be automatically submitted
- Vendor influence: A unified voice to influence industry vendors
- Online Community: Privileged access to our online community

Visit **Cyber Executive Forum** for more information or to register for the Forum

CHAPTERS LIST

Asia Pacific

Bangladesh
Chennai
Dehradun
India
Philippines

Canada

Alberta
Ottawa
Quebec City
Vancouver

Europe

Brussels European
France
Germany
Italy
Netherlands
Poland
Romania
Spain
Switzerland
Turkey
UK
Ukraine

Latin America

Argentina
Barbados
Bolivia
Brasil
British Virgin Islands
Chile
Columbia
Ecuador
Peru

Middle East

Bahrain
Egypt
Iran
Israel
Kazakhstan
Kuwait
Qatar
Saudi Arabia

USA

Alamo San Antonio
Blue Ridge
Boise
Buffalo Niagara
Capitol of Texas
Central Alabama
Central Florida
Central Indiana
Central Maryland
Central New York
Central Ohio
Central Plains
Central Texas
Central Virginia
Charleston
Charlotte Metro
Chattanooga
Chicago
Colorado Springs
Columbus
Connecticut
Dayton
Delaware Valley
Denver
Des Moines

East Tennessee
Eastern Idaho
Eugene
Fayetteville/Fort Bragg
Fort Worth
Grand Rapids
Grand Traverse
Greater Augusta
Greater Cincinnati
Greater Spokane
Hampton Roads
Hawaii
Inland Island
Kansas City
Kentuckiana
Kern County
Lansing
Las Vegas
Los Angeles
Metro Atlanta
Mid-South Tennessee
Middle Tennessee
Milwaukee
Minnesota
Motor City

National Capital
New England
New Hampshire
New Jersey
New York Metro
North Alabama
North Dakota
North Oakland
North Texas
Northeast Florida
Northeast Indiana
Northeast Ohio
Nothern Colorado
Northern
Virginia (NOVA)
Northwest Arkansas
Northwest Ohio
Oklahoma
Oklahoma City
Orange County
Phoenix
Pittsburgh
Portland
Puerto Rico
Puget Sound (Seattle)

Quantico
Rainier
Raleigh
Rochester, NY
Sacramento Valley
San Diego
San Francisco
Silicon Valley
South Bend - Michiana
South Florida
South Texas
Southeast Arizona
Tampa Bay
Tech Valley of New York
Texas Coastal Bend
Texas Gulf Coast
Triad of NC
Triad of SC
Utah
Ventura County
West Texas
Wyoming
Yorktown