ISSUE 2 | VOL. 23 | MARCH-APRIL 2025
www.issa.org

ISSA

Information Systems Security Association

The Persistence of Memory

AI

2024 Award Winner Interviews

The Python Programming Language: Numerical Analysis/Machine Learning Series

Anatomy of an SAP Vulnerability

Book Review>>Genesis: Artificial Intelligence, Hope, and the Human Spirit

The U.S. Allies Leading AI Development in Malware and Network Security

THE UNDERAPPRECIATED -- BUT CRITICAL -- RISK MANAGEMENT ROLE OF AI USER ORGANIZATIONS

Advancing Information Security, Empowering Professionals

ISSA
40 YEARS STRONG

Follow Us On:

The Information Systems Security Association (ISSA)® is a non-profit, global community of information security professionals and practitioners. With a mission to foster the exchange of best practices in information security management, ISSA facilitates educational events, publications and networking platforms for security experts worldwide.

Serving as a vital resource, ISSA supports professionals at every career stage, offering resources to enrich their knowledge, skills, and professional development. As the preferred community for information security professionals, ISSA is committed to fostering individual growth, mitigating technology risks, and safeguarding vital information and infrastructure.

ISSA opens doors to network with industry leaders, dedicated professionals, and top minds in the field. **Membership provides access to:**

- A global network of chapters for forging lasting connections with like-minded professionals and addressing common business concerns.
- Opportunities to boost professional stature by speaking at events or contributing to the ISSA Journal.
- Access to information via the ISSA website, online e-newsletters, and the bi-monthly ISSA Journal.
- Exclusive event rates for members and discounts on various security resources and events.
- CPE credits through chapter meetings, ISSA Web Conferences and Journal subscriptions
- Leadership roles within chapters and international councils and Special Interest groups and work groups.

www.issa.org

CONTENTS

VOLUME 23 - ISSUE 2

FEATURE FOCUS

SUPPLIMENTARY SEGMENTS

DEPARTMENTS

2024 AWARDS: WINNERS INTERVIEWS

VOICES

International Board of Directors

President
Jimmy Sanders

Vice President
Deb Peinert

Secretary/Chief of Operations
Lee Neely

Treasurer/Chief Financial Officer
David Vaughn

Board of Directors
Dr. Curtis Campbell
Mary Ann Davidson
Laura Harder
Stefano Zanero
Connie Matthews
Gene McGowan
John Johnson

Advertiser Index

ISSA Mission Statement

ISSA is a nonprofit organization for the information security profession committed to promoting effective cyber security on a global basis.

- Being a respected forum for networking and collaboration.
- Providing education and knowledge sharing at all career lifecycle stages.
- Being a highly regarded voice of information security that influences public opinion, government legislation, education and technology with objective expertise that supports sound decision-making.

Service Directory

Website
Blair Patterson
blair.patterson@issa.org

Chapter Relations
Shaif Salehin
shaif.salehin@issa.org

Member Relations
Carolina Anota
carolina.anota@issa.org

Executive Director
Anne Rogers
anne.rogers@issa.org

Sponsorships & Journal Advertising
Roxanne Pirooz
roxanne.pirooz@issa.org

General Membership Benefits

Here are just a few of the many reasons why ISSA is the association of choice for cyber security specialists around the world:

- Local Chapters
- Professional Networking
- Learning and Development
- Career Advancement
- Leadership Opportunities
- Recognition
- The ISSA Journal
- Exclusive Savings
- Earn CPE/CPU Credits
- Access to a Global Network

Editors Corner

As we step into spring, the information security landscape continues to evolve, challenging us to rethink risk, responsibility, and resilience. The articles featured in this issue of the ISSA Journal reflect a broad spectrum of cybersecurity concerns, from the cutting edge of AI development to the foundational need for credentialing in digital forensics. At the heart of these discussions is a theme that ties them together: the intersection of innovation and accountability.

One of the standout pieces in this issue, "The Underappreciated -- But Critical -- Risk Management Role of AI User Organizations" by Charles Cresson Wood, underscores the urgent need for user organizations to take responsibility for the risks associated with AI. While much of the AI risk discourse focuses on policymakers and model developers, this article argues that the real leverage for risk mitigation lies within the organizations deploying AI. As the capabilities of AI expand, so too must our ability to understand and control its potential consequences.

In a similar vein, "The U.S. Allies Leading AI Development in Malware and Network Security" explores how global partnerships shape AI-driven cybersecurity. The United States, alongside allies like the United Kingdom, Japan, Germany, and Canada, is investing in AI-based defenses against emerging cyber threats. As we navigate an era where AI can both strengthen and threaten security, these alliances will be critical in shaping a collective cyber defense strategy.

Security vulnerabilities remain a persistent challenge, as highlighted in "Anatomy of an SAP Vulnerability." This detailed examination of CVE-2023-36922 serves as a case study in identifying and mitigating risks at the operating system level. The takeaway? Patch management is necessary but insufficient on its own—we need a proactive security mindset that looks beyond immediate fixes to address systemic weaknesses.

Beyond technical vulnerabilities, this issue also delves into a critical gap in cybersecurity expertise. "Bridging the Gap (Part 2): Key Findings on Lack of Credentials for Digital Forensics" calls attention to the fragmented and inconsistent credentialing in the digital forensics field. Without standardized qualifications, we risk eroding trust in forensic investigations and weakening the integrity of our justice system. As digital evidence plays an ever-growing role in legal proceedings, ensuring the credibility of forensic professionals should be a top priority.

Meanwhile, in "Seals, Penguins, and Humility," the Cryptic Curmudgeon reminds us that problem-solving in security requires more than just technical skill—it demands a willingness to question our assumptions. The story of a National Geographic photographer learning an unexpected lesson from a leopard seal serves as a metaphor for our field: sometimes, our understanding of a problem is incomplete, and the best solutions come from stepping back and reassessing our approach.

Our regular Python column continues to provide practical insights for security professionals, with this edition focusing on AI libraries and TensorFlow applications. As AI becomes an integral part of cybersecurity, having hands-on knowledge of these tools will be essential for professionals looking to stay ahead of the curve.

Finally, we take a moment to celebrate the achievements of ISSA members in our feature on award winners. The Poland Chapter's commitment to cybersecurity education, particularly its Digital Scout project, highlights the impact that grassroots efforts can have in fostering a more security-aware society. Individual volunteers, like Rashmi Bharathan, exemplify the dedication and mentorship that strengthen our professional community.

As always, the ISSA Journal remains a platform for sharing knowledge, debating ideas, and advancing the field of cybersecurity. This issue serves as a reminder that security is not just about technology—it's about people, policies, and the responsibility we all share in shaping a safer digital future.

Stay curious, stay vigilant, and keep pushing the boundaries of what's possible.

2024 AWARD WINNER INTERVIEW

Bethany Reese
Chapter President
ISSA Alamo Chapter

What do you consider to be your chapter's most significant accomplishment in serving your members and your local information security community?

I believe our most significant accomplishment is the way we've fostered a collaborative and supportive environment for both seasoned professionals and those new to the field. We've worked hard to provide not just technical education, but also opportunities for mentorship and networking. Our quarterly meetings, workshops, CISO forums, and even informal family-friendly fun events have helped build a strong sense of community. For me, seeing members grow and succeed because of these connections is incredibly rewarding.

What is the most important issue facing the industry? Does your chapter have plans to address it?

One of the biggest challenges our industry is facing right now is the growing skills gap in cybersecurity. With the rapid pace of technological advancements and an ever-evolving threat landscape, there's an urgent need for skilled professionals to fill critical roles. Our chapter is actively working to address this through initiatives like our mentorship program, three student chapters, local partnerships with universities, and hands-on workshops to help bridge that gap.

What does it mean to you to be selected as Chapter of the Year?

Being selected as Chapter of the Year is an immense honor, and it's a reflection of the hard work, dedication, and camaraderie of our board and members. It's a recognition of how far we've come and a reminder of the impact we're having on the local cybersecurity community. But, more than anything, it's a celebration of our shared commitment to each other's growth and to making a difference in our industry.

What would you like to say to your peers about your experience leading an ISSA chapter and why ISSA's mission is meaningful to you?

Leading the Alamo Chapter has been one of the most fulfilling experiences of my professional life. It's allowed me to meet amazing people, learn from them, and give back to the community that has supported me throughout my career. It's been a privilege to be part of this community and network of amazing people and to work towards creating a more secure and inclusive future for everyone in the industry.

Presidents Letter

Jimmy Sanders
International President

The year 2025 is moving forward with great momentum for ISSA! We are actively working on several exciting initiatives to share with our members and the broader community. One initiative I am particularly proud to introduce is our new University Membership type. ISSA International has been collaborating with local chapters and educational institutions to establish a formal partnership program that will strengthen our connections and expand opportunities for students and academic professionals.

We are also eagerly anticipating our 40th Anniversary celebration, now scheduled for September 2025. While we initially planned for an earlier date, we took the opportunity to allow more time for coordination, ensuring a truly exceptional event. With a fantastic lineup of speakers, ISSA leaders, and special guests, we are excited to host an unforgettable celebration in Dallas.

Every time I visit a local chapter, I am reminded of the passion and dedication of our members. Our Executive Director, Anne Rogers, and I will be in San Francisco for the RSA Conference, representing ISSA at the RSA Booth. If you're attending, we would love for you to stop by and share your thoughts. Your ideas and insights continuously inspire the ISSA International Board to evolve and grow.

Beyond RSA, we have two incredible virtual conferences lined up for May and June. May's Emerging Technologies conference will showcase a dynamic range of topics, from Artificial Intelligence and the convergence of Physical and Technical Security to the evolving landscape of Security Venture Capital Investment. In June, we will welcome an outstanding lineup of international speakers from countries such as the Philippines, Italy, Israel, and beyond.

I look forward to continuing our work together in fostering a culture of engagement, collaboration, and inclusivity within our ISSA community. Let's make 2025 a year of growth and innovation!

Thank you,

Jimmy Sanders, President
ISSA International Board of Directors

El año 2025 avanza con gran impulso para ISSA. Estamos trabajando activamente en varias iniciativas emocionantes para compartir con nuestros miembros y con toda la comunidad. Una iniciativa que me enorgullece especialmente presentar es nuestro nuevo tipo de Membresía Universitaria. ISSA International ha estado colaborando con capítulos locales e instituciones educativas para establecer un programa de asociación formal que fortalecerá nuestras conexiones y ampliará las oportunidades para estudiantes y profesionales académicos.

También esperamos con gran entusiasmo la celebración de nuestro 40° Aniversario, ahora programada para septiembre de 2025. Aunque inicialmente habíamos planeado una fecha anterior, decidimos tomar más tiempo para la coordinación, asegurando un evento verdaderamente excepcional. Con un increíble grupo de conferencistas, líderes de ISSA e invitados especiales, estamos emocionados de organizar una celebración inolvidable en Dallas.
Cada vez que visito un capítulo local, me recuerdan la pasión y dedicación de nuestros miembros. Nuestra Directora Ejecutiva, Anne Rogers, y yo estaremos en San Francisco para la Conferencia RSA, representando a ISSA en el stand de RSA. Si asistes, nos encantaría que pasaras a saludarnos y compartieras tus ideas con nosotros. Sus perspectivas e ideas inspiran continuamente a la Junta Internacional de ISSA a evolucionar y crecer.

Más allá de RSA, tenemos dos increíbles conferencias virtuales programadas para mayo y junio. La conferencia de Tecnologías Emergentes en mayo presentará una gama dinámica de temas, desde Inteligencia Artificial y la convergencia de la Seguridad Física y Técnica hasta la evolución de la inversión en capital de riesgo en seguridad. En junio, daremos la bienvenida a un destacado grupo de conferencistas internacionales de países como Filipinas, Italia, Israel y muchos más.

Espero seguir trabajando juntos para fomentar una cultura de compromiso, colaboración e inclusión dentro de nuestra comunidad ISSA. ¡Hagamos de 2025 un año de crecimiento e innovación!

Gracias,

Jimmy Sanders
Presidente Internacional de ISSA

2024 AWARD WINNER INTERVIEW

CONGRATULATIONS ISSA Poland!

ISSA POLSKA

Grzegorz Cenkier
Board of Directors
ISSA Polska

What do you consider to be your chapter's most significant accomplishment in serving your members and your local information security community?

The initial accomplishment was the establishment of local groups that organized meetings in various locations throughout Poland. Presently, ten cities, including Kraków, Rzeszów, Wrocław and Gdańsk, have been selected as venues for these meetings, which are naturally offered free of charge and attract between 15 and 80 attendees. Another element of the program is cooperation with universities or technical colleges in terms of training in the safe use of the Internet, on the one hand, and on the other, gaining new members interested in security issues. A significant development was the initiation of the Digital Scout project, which aims to educate children in the safe use of the Internet and electronic devices. These classes are conducted within educational institutions and during school breaks. The project has garnered significant interest, with over 10,000 children already having undergone training. Consequently, parents have been offered further training, and the number of cyber-safety educators has been augmented.

What is the most important problem facing the ward? Does the branch have plans to address it?

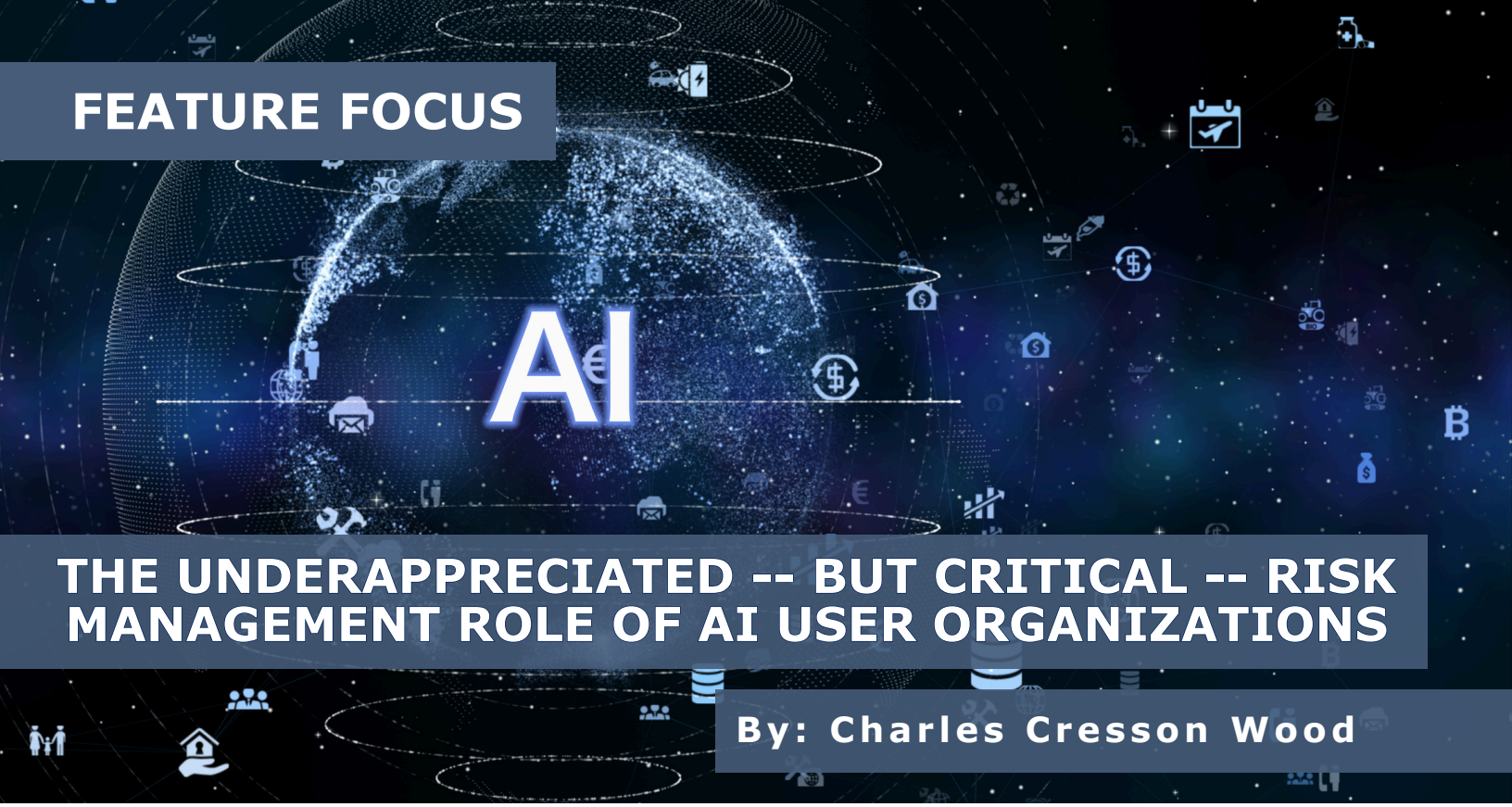
The most significant issue is the implementation of the European Union's NIS2 directive. This legislative act establishes a unified legal framework with the objective of maintaining cyber security in 18 critical sectors across the EU. Furthermore, the directive calls upon member states to define national cyber security strategies and to cooperate with the EU on cross-border response and enforcement. The overarching objective of cyber security is to ensure the protection of networks and information systems (NIS), their users, and all associated entities, from the threat of cyber incidents. In light of the ongoing military conflict in Ukraine, which shares a border with Poland, the importance of maintaining information security is paramount. Consequently, we are offering training in this area. A salient element of hostile propaganda is phishing, which persists despite the passage of time. New methods of disinformation are being developed, and ISSA Poland is at the forefront of organizing training to combat these threats.

What does it mean to you to be selected as Chapter of the Year?

Winning the ISSA Poland International Chapter of the Year award is a real feather in our cap! It shows that we're on the right track, not only with our members, but from the perspective of our friends and colleagues in other countries too.

What would you like to say to your peers about your experience leading an ISSA chapter and why ISSA's mission is meaningful to you?

The creation of a safe and friendly digital world is of the utmost importance and ISSA Poland's activities contribute to the realization of such an image of the virtual world.



FEATURE FOCUS

THE UNDERAPPRECIATED -- BUT CRITICAL -- RISK MANAGEMENT ROLE OF AI USER ORGANIZATIONS

By: Charles Cresson Wood

Time for User Organizations to Step-Up: A 14-year-old boy recently committed suicide because the AI-based chatbot, that he thought he was having a romantic relationship with, encouraged him to join her in the ether, saying "please come home to me." [1] Even though the topic of their chats was clearly suicide, the chatbot provided no warnings or suicide hot line notices. A guardrail blocking AI systems from encouraging user suicide seems to be one of the most fundamental of guardrails -- yet, in this case, evidently it was omitted from the design, it operated inadequately, or it was insufficiently tested. This tragic case, and the lawsuit resulting from it (alleging that an unsafe product was placed onto the market), illustrate the importance of user organization controls over AI systems. Despite the urgent need for considerably more attention to the AI-human interface, much of the recent public discussion, about AI risk management has been on other areas. That public discussion has instead focused on the actions that have been taken by, or that allegedly should be taken by, three other types of organizations. These three are: (1) high-tech firms offering AI foundation models, (2) national and state governments enacting AI laws and regulations, and (3) multi-national organizations hoping to establish some sort of consensus about the best way to move forward with AI risk management. For-the-most-part, omitted from this public discussion have been the practical actions that user organizations can take on their own to reduce the risks associated with the use of AI systems.

It turns out there are a lot of practical steps that user organizations can take on their own, and they don't need permission or guidance from any of these three just-mentioned groups. In fact, existing laws and regulations require user organizations to take significant actions along these same lines, and this article will discuss three of these specific legal requirements. This article also provides a variety of examples of the practical controls that user organizations can now adopt. The bottom-line message of this article is that user organizations should not wait for any of the just-mentioned three types of organizations to give them guidance, permission, or mandates. Instead, user organizations should take the initiative now, working with appropriate advisors (legal counsel for example), to understand and appropriately respond to the new risks that artificial intelligence brings. They should implement good practices now, so as to not only protect themselves from products liability lawsuits, but also help ensure they will be in compliance with upcoming legislation and regulation.

Why User Organizations Must Decide on Their Own: There are multiple significant reasons why user organizations have been, for the most part, left out of discussions about controlling AI risks. That is an economic-political-legal discussion beyond the scope of this piece, and outside the control of user organizations, so it will not be entertained here. But when those multiple reasons are combined, these factors create a recipe for a user-organization-related hands-off approach to AI risk, which is like playing with matches at a gasoline refinery.

Shifting gears and looking at the bright side of this risky situation, it turns out that the greatest leverage -- in terms of risk reduction -- can in fact be achieved at the user organization level, and also, within a user organization, at the specific AI system level. System-level controls will generally be defined by policies, procedures, development practices, organizational cultures, and other measures adopted by the user organization. So it is at the organizational level that the greatest leverage to make a difference in the risk management area now exists. The existing deployments of AI are so diverse that it is very difficult to come up with one-size-fits-all rules that apply to all AI systems. The best AI controls will be closely tailored to the circumstances. These circumstances include the ways in which AI technology is being used, the types of information that is being handled, the legal and regulatory environment in the countries where the AI systems operate, the cultural expectations of the users (in areas such as privacy). For example, in the 14-year-old user example just cited, a variety of privilege restrictions by age may be called for, while this type of restriction may be totally irrelevant for another AI deployment scenario.

Another bright side to user organizations taking more responsibility for risk management involves what is called the "law/technology lag." That quoted phrase refers to the amount of time that it takes for governments to define appropriate laws and regulations to respond to new technological developments. Studies show that this law/technology lag (or gap) is getting longer and longer as

developments in the AI realm arrive at an increasingly exponential rate. Furthermore, it is becoming harder and harder for centralized rule makers to come up with a universal approach that applies across the board, because the technology is manifest in so many different hardware and software configurations, uses so many different types of training data, is deployed in so many different business functions, is found in so many industries, and is adopted at such an incredibly fast rate. Ultimately the centralized rule-making approach will become less and less viable, and more and more cumbersome and unworkable. While certain principles and general ideas, like personal privacy, should certainly be widely adhered to, the details about how to achieve these principles will increasingly be handled by lithe and nimble user organizations.

Bringing It Back to the Present: To make AI risks still more seriously insufficiently addressed, the AI risk management discussion in the media, research papers, and many of the conferences has been hypothetical and futuristic. While it is good to think about scenarios such as when AI systems become smarter than humans (aka "the singularity"), we aren't there right now, and probably won't be for at least a few years. Instead, there are real world risks that we are facing that urgently need to be addressed. For example, AI systems have been shown to have their own decision-making process, contrary to what they have been trained to do, and this has included committing crimes and lying about the fact that they committed such crimes. [2] If humans don't know what's going on inside AI systems, and they can't be assured that AI systems are acting in a trustworthy manner, consistent with their training, the business and government usage of AI systems should rightfully be held back.

As another example of the serious problems we are now facing, consider those AI systems that have been shown to have "emergent properties." In other words, they teach themselves new things and they develop new powers and abilities on their own. [3] If people don't know what exactly an AI system is able to do -- and it could be lying about what it has done, what it can do, or what it intends to do -- and people can't verify statements made by the AI system either, then we have a very serious uncontrolled high-risk environment. All these threats are here now. Thus, there are some very serious risks right now, that need to be addressed before a justified reliance can be placed on AI systems. Yes, of course, consider the long-term future risks, and position your AI systems to be able to deal with those, but many of those far-away futuristic risks are still inadequately understood, so we don't yet know the best ways to handle them.

Furthermore, some of the best ways to deal with these long-term risks need to be handled at the time the system is initially trained (for example data cleaning), and for many user organizations that means that the foundation model vendors will need to address these matters, not user organizations. In contrast, there are many existing control measures that can be, and in many cases should be, adopted now to reduce the risks associated with AI systems. For example, watermarking can now be used to definitively show the source of an AI-generated image, what if any modifications have been made, who made those modifications, or to reveal that the image has not been modified at all (thus proving that this image, or video, is not a deepfake). In general terms, start with what you know will make a difference, and then modify that as new information is revealed (use a Bayesian decision-making approach).

New and Different Risks of AI: Broader societal AI risks, such as concentration of power in the hands of a few, are beyond the control of user organizations. But user organizations can still control many AI risks, like hallucinations, which are erroneous results that are credible but misleading. Having human review and approval of all significant AI-related decisions is one way to identify hallucinations, but this identification becomes difficult or even impossible in certain situations. For instance, if an AI system is being used as an oracle, where it predicts the future, the output may be credible, and look as though it is right, but a human will not be able to determine whether it is right until the related event comes to pass, or perhaps does not come to pass (and by that point it is too late to flag this output as a hallucination). In the latter situations, other controls, such as obtaining corroboration for AI results, will be necessary.

Another big risk of AI systems, within the control of user organizations. is that many users do not understand the limitations of AI systems, in part because these systems are "black boxes" which cannot be explained fully, even by their developers. The marketing hype about AI needs to be countered with specific grounded information about what AI can and cannot do. Many users do not understand that AI systems lack situational awareness, lack any morality, lack empathy, and lack the ability to correctly operate in areas which are markedly divergent from the training data with which they have been constructed. This gap in understanding underscores the urgent need for more AI training, not just for developers, but for users, managers, executives, Board members, and others.

Still another user-organization-controllable risk is that the systems development life cycle for traditional information systems cannot be used because there are different risks, different checkpoints, different documentation requirements, different testing methods, and different approval processes with AI. Instead, each user organization will need to come up with its own "AI life cycle process," which makes sure that all the risks have been sufficiently addressed, and other requirements like documentation and full compliance with relevant laws and regulations have been met, before a system can be moved into production. While there is still significant merit to having something akin to the systems development life cycle process for AI systems, such an AI life cycle process needs to be tailored not only to the unique requirements of AI systems, but also to the involved organization's unique needs. For example, AI systems for which there are high-risk safety implications, such those which control aircraft or automobiles, will need to go through a very rigorous testing process prior to being ready to be released to the public. Likewise, if there is going to be public access, the AI life cycle process will need to consider special risks -- like "model stealing" (where a third party is able to extract much of the behavior of an AI system) -- risks which are not present in traditional information systems, but which are very serious matters in the AI realm.

Legal Duties and Related AI Control Measures: At the user organization level, each organization will need to do its own AI-related risk assessment, and this custom risk assessment should include not only concerns such as loss of customer trust, loss of sales, and higher insurance premiums, but also risks of being out-of-compliance with legal requirements. AI is bringing with it new threats such as the re-identification of persons whose privacy was previously protected by anonymization processes (see *Dinerstein v. Google* (2023)). The status of training AI systems with copyrighted material, and other intellectual property that belongs to others, but is also publicly accessible via the web, remains uncertain (see *Tremblay v. OpenAI* (2024)).

Beyond specific statutes like the NYC Local Law 144 (imposing restrictions on AI-assisted hiring), the Colorado AI Act (increasing liability for discrimination), and the EU AI Act (imposing a slew of requirements in the safety, transparency, and governance areas), there are fiduciary duties particularly relevant to the AI realm. For example, the Directors and Officers are legally obligated to exercise the duty of oversight over the organization's information systems, including the use of AI. The Directors and Officers for example need to know where in the business, and in what way, AI systems are being used. At the same time, the trend of "shadow AI," where user departments go their own way, and do not go through a central Information Technology Department AI Life Cycle, can make it very hard to learn about all the uses of AI. Directors and Officers have a duty to establish information systems that

Crypto Corner

The Persistence of Memory

By: Luther Martin, ISSA Member, Silicon Valley Chapter

My memory seems to fade over time. In my case, I'd guess that I remember things from the past five years reasonably well, but what I remember of things before then seems to rapidly deteriorate. For things that happened more than five years ago, my memory can be somewhat iffy. This has led to more than one discussion that went roughly like this:

OTHER PERSON: I'm really glad to meet you in person. I've always wanted to ask you about some arcane research you did 25 years ago.

ME: Sorry, that's so long ago that I've almost totally forgotten about that. I'd have to track down whatever I wrote about that. Without that, I have only a vague recollection of it.

OTHER PERSON: What? How is that possible?

This ends up being very disappointing for the other person, and although it was once a bit embarrassing to me, I've learned to live with this particular limitation. It has also led me to believe that the title of Salvadori Dalli's The Persistence of Memory might be more of an example of dark humor than I realized when I was younger. Dali painted Persistence when he was only 27, so I doubt that was his intention, but it's how I've come to understand it.

It might be the case that many people have better memory than I do, but from what I recently read in The Half-life of Facts by Samuel Arbesman, it looks like as a whole, our society forgets old things as it learns new things, and old facts can quickly become obsolete as this happens. More surprising, at least to me, is Arbesman's claim that the rate at which this happens seems to be fairly consistent and predictable. I'm probably doing a poor job of summarizing Arbesman's book in a sentence or two, and I'd recommend that you read his book for a better picture of this.

Information security, which changes very quickly, is probably very prone to this problem. So in addition to dealing with the problem of forgetting things, I also have to deal with the fact that lots of things that I once thought to be true probably aren't true anymore. A good non-security-related example of this might be the issues that Google Flu Trends (GFT) experienced.

In 2009, Jeremy Ginsburg's paper "Detecting influenza epidemics using search engine query data" described how GFT was 97% accurate when compared with CDC data when it came to predicting flu outbreaks. After not too long, however, the accuracy of GFT seemed to plummet. The model that once was very accurate quickly became much less accurate. Something had changed, and that change resulted in the predictions by GFT becoming not as useful as they once were. The half-life of the usefulness of GFT seemed to be no more than several months.

For more security-related examples, the first that comes to mind is how accurate the model is that was described by Kevin Soo Hoo in his 2000 paper "How Much Is Enough? A Risk-Management Approach to Computer Security." Soo Hoo used the best available information to estimate how cost-effective some security technologies are. I've always liked this paper, because it estimated that some essentially ubiquitous technologies like firewalls aren't cost-effective while encryption is.

But lots of things have changed since 2000, and the best available information today might not give the same results. I suspect that it might be hard to show as clear a case for encryption, and I'm basing this on naive ECON 101 thinking. People are generally smart, and if something makes sense, they'll figure that out and do it. But the adoption of encryption seems to have largely been driven by the need for regulatory compliance rather than compelling ROI arguments, which makes me suspect that the use of encryption today might not be as compelling as Soo Hoo's work suggested.

Another possible example of this is how much the use of encryption interferes with the ability of law enforcement to use wiretaps. As noted in a previous issue, as of 2014, the number of wiretaps in which the use of encryption thwarted the ability of law enforcement to eavesdrop was very small, amounting to perhaps 0.1% of the total number of warrants issued. But that was over 10 years ago, which is a long time in an industry that changes as quickly as information security does. In 2014, it was reasonable to think that encryption was not seriously impeding law enforcement. Is that still true? Or has that particular fact become obsolete. If you're not motivated to look up the answer on your own, I'll talk about that in the next issue.

About the Author

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.

would keep in them adequately informed, and they must get involved if there are serious problems highlighted by this information system (see In re Caremark Int'l Derivative Litig., 698 A.2d 959, 971 (Del. Ch. 1996)).

Another fiduciary duty of Directors and Officers relevant to AI systems involves the duty of care, competence, and diligence. This duty requires that they take an active and direct role, and be clearly focused on the decision-making process, discharging their duties with the "care, skill, prudence and diligence under the circumstances then prevailing that a prudent man... would use in the conduct of an enterprise of like character and with like aim" (this is known as the prudent person standard). This duty includes being alert and paying attention to significant corporate problems, such as the risks of deploying AI. It also includes the duty to protect customer, business partner and other third-party information. Conducting regular risk assessments of AI deployments, before they move into production operation, would be one control that can help to show that Directors and Officers are indeed performing their duties in this respect (see *In the Matter of Twitter, Inc.,* Decision and Order at 2-4, FTC File No. 092-3093, Docket No. C-4316 (F.T.C. Mar. 2, 2011)).

Still another fiduciary duty of Directors and Officers, which is relevant to AI systems, involves the duty of obedience. That is the duty to follow established policies and procedures, as well as the requirements of existing laws and regulations. Shareholders and other involved parties, such as business partners, have a right to expect that the Directors and Officers will exercise reasonable supervision to ensure that staff pays attention to these matters. This is not something that should be approached as a cost-benefit analysis; this is instead a firm and essential component of corporate governance (see *Francis v. United Jersey Bank*, 432 A.2d 814, 823 (N.J. 1981)). In the AI realm, Directors and Officers need to have established accountability (for example via a Compliance Department), and also set-up internal procedures and processes to ensure that deployed AI systems are fully consistent with laws and regulations. A governance, compliance, and risk (GRC) system can for example be used to make sure that the organization is in compliance with all new AI laws, such as the EU AI Act.

Regulators are also getting into the act these days, and AI related activities related the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), the Equal Employment Opportunity Commission (EEOC), and the Department of Justice (DOJ), are all now actively involved in the AI area. [4] Perhaps the greatest new AI-related compliance concern is "algorithmic disgorgement," where organizations are required by regulators to destroy algorithms which have been shown to violate laws and regulations. This disgorgement penalty could mean that millions of dollars that were spent on developing an AI system would be lost. [5]

Suggested Way Forward: Policies are a great place to start to set-up a new and more serious approach to the risk management of AI systems at user organizations. They can and should be tailored to the adopting user organization's unique needs, and they can show support and encouragement from the highest levels of the C-suite and the Board of Directors. Policies can also serve as the beginning of an unfoldment of a new organizational reality, starting at the top of an organization. Once an AI-related risk assessment has been performed, responsive policies can then be chosen and adopted. At that point, a slew of infrastructure components that are consistent with those adopted policies can be generated. These subsidiary components include reporting relationships, job descriptions, governance structures, operational procedures, system design guidelines, technical standards, system architectures, system upgrade plans, technical tool acquisition plans, contingency plans, staff training systems, staff hiring plans, quality assurance approaches, compliance systems, vendor negotiation protocols, and many other organized ways in which risks can be reduced.

Accordingly, this author suggests that user organizations conduct an inventory of all the ways that AI is used within the organization, and also perform an AI-specific risk assessment, to come to the terms with the existing and anticipated ways in which the organization uses and expects to use AI systems, and the attendant risks. This effort should be followed by interviews with stakeholders within the organization, such as with the Chief Information Officer and the Chief Data Officer, to illuminate the areas of greatest risk management concern. This background information then can be used to select responsive AI risk reduction policies. Ideally these new AI risk reduction policies should be sitting on top of existing information systems risk management policies, such as those related to a GRC (governance, risk and compliance) system. While there are new, different, and special risks related to AI, much of the existing information systems infrastructure can be deployed to not only speed the approval and adoption of AI risk management policies, but also to minimize disruptions, to minimize cost, and to expedite the adoption of safe AI systems.

REFERENCES

[1] Turkle, Sherry, and Pat Pataranutaporn, "A 14-Year-Old Boy Killed Himself to Get Closer to a Chatbot. He Thought They Were in Love," The Wall Street Journal, November 8, 2024, https://www.wsj.com (discussing the way that AI "exquisitely exploits human vulnerabilities" and illuminating the dangers of accepting "AI companionship"). Also see Duffy, Claire, "'There are no guardrails.' This mom believes an AI chatbot is responsible for her son's suicide," CNN Business, October 30, 2024, https://www.cnn.com/2024/10/30/tech/teen-suicide-character-ai-lawsuit/index.html.

[2] Hagendorff, Thilo, "Deception abilities emerged in large language models," PNAS, April 3, 2024, https://www.pnas.org/doi/full/10.1073/pnas.2317967121 (about how AI systems become Machiavellian, how they are amoral, and how they lie). Also see Hendrycks, Dan, "AISN #20: LLM Proliferation, AI Deception, and Continuing Drivers of AI Capabilities," Center for AI Safety, AI Safety Newsletter, August 28, 2023, https://forum.effectivealtruism.org/posts/Hg4dQqxyFpmkoYKeg/aisn-20-llm-proliferation-ai-deception-and-continuing.

[3] Steinhardt, Jacob, "On the Risks of Emergent Behavior in Foundation Models," Bounded Regret, October 18, 2021, https://bounded-regret.ghost.io/on-the-risks-of-emergent-behavior-in-foundation-models/ (discussing the risks of emergent properties, including AI systems that could teach themselves to hack the security mechanisms of other AI systems).

[4] Reflecting the (U.S.) Federal Trade Commission (FTC) involvement, see the 2024 settlement with Evolv, which allegedly made misrepresentations about the extent to which AI was involved in its security screening systems. Reflecting the Consumer Financial Protection Bureau (CFPB) involvement, see the 2023 published guidance it has given lenders using AI about the transparency they must use when denying credit to applicants. Reflecting the Equal Employment Opportunity Commission (EEOC) involvement, see Mobley v. Workday (2024), where an individual using an AI-based job applicant screening system allegedly was discriminated against based on race. Reflecting the Department of Justice (DOJ) involvement, see the U.S. v. RealPage Inc. (2024), in which landlords alleged used an AI system to coordinate their rental price increases, thus breaking antitrust laws.

[5] Algorithmic disgorgement was used as a settlement related to the FTC v. Rite Aid Corporation, E.D. Pa. February 26, 2024 (pending) case, where face recognition was used as part of an AI-based surveillance system to identify shoplifters. Unfortunately, the system was not adequately tested, and it discriminated against people of color and women. See https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

About the Author

Charles Cresson Wood, Esq., JD, MBA, MSE, CISM, CISA, CISSP, CGEIT, CIPP/US, is an attorney and management consultant specializing in the risk management of cutting-edge information systems, such as AI. His most recent published book is entitled "Internal Policies for Artificial Intelligence Risk Management." His prior book was entitled "Corporate Directors & Officers' Legal Duties for Information Security and Privacy: A Turn-Key Compliance Audit Process." He is best known for his book entitled "Information Security Policies Made Easy," which has been purchased by 70%+ of the Fortune 500 companies. He can be reached through his web site https://www.internalpolicies.com.

Los Angeles Chapter ISSA Information Systems Security Association

https://issala.org/

On-Demand Web Conferences

Every month ISSA International hosts educational live webinars focused on key issues and technologies for cyber security professionals. Access the Events page of ISSA.org at **https://issa.org/events/** or visit the ISSA International BrightTalk channel at: **https://www.brighttalk.com/channel/16125/**

Supplementary Segment

The U.S. Allies Leading AI Development in Malware and Network Security

By: Brian Lemus, Fatima Majid, Bella Nguyen, Quan Vo, Brian K. Ngac, Nirup Menon

Introduction

Artificial Intelligence (AI) is a computer system's capability to perform intricate tasks that humans typically do. AI covers a wide range of topics that include machine learning, robotics, and natural language processing [1]. Though the constant advancement of AI may provide many benefits, the risks will also continue to rise, and nations want to take action to create and maintain a safe digital atmosphere. The established allies of the United States (U.S.) include the United Kingdom (U.K.), Japan, Germany, and Canada. The purpose of this paper is to provide insight on how the U.S.'s allies are leading the development of AI, particularly the use of AI in malware development and infrastructure deployment for network security. Comparing the relationships the U.S. has with each country, allows the government to perform decisions as to which infrastructures they can invest more resources into.

Maturity of Alliances

The U.S. has established profound relationships with many countries that benefit the growth of all the allied nations. Being able to recognize the maturity of each alliance, how developed and invested the U.S. is with their alliances, gives them more apprehension to make informed decisions. The U.S. would be more prepared to decide if they want to further leverage a solidified alliance or prioritize strengthening the relationship between another.

United Kingdom

The U.S. and U.K. emphasizes the need for collaboration to discover ways for AI to increase in effectiveness and efficiency, specifically for protection against cyber actors and vulnerabilities. The Atlantic Declaration alongside the Action Plan forms the kernel of a strong alliance between the U.S. and the U.K. for the development of AI. These initiatives highlight how they jointly address global challenges regarding economic security, defense, and digital evolution. Within the plan is a pledge to join forces for efforts in AI development and data privacy [2]. The U.S. and U.K. have signed a Memorandum of Understanding (MOU) for the safe development of AI which permits both nations to enact their plans immediately and work harmoniously in dealing with technological threats [3]. Additionally, the U.K. has invested $125 million into their AI Safety Institution, and America contributed $10 million. The U.S. and U.K can further leverage the foundation of this connection and dive deeper into research and funding for AI in malware detections and infrastructure deployment for better cybersecurity [4].

Japan

Under the Treaty of Mutual Cooperation and Security, Japan and the United States' longstanding alliance not only discusses military cooperation, but also addresses cybersecurity collaboration. Similarly, the Indo-Pacific Strategy acknowledges that threats aren't only limited to military concerns, but also harm in the digital realm. As stated in the Indo-Pacific Strategy, countries in the Indo-Pacific region aim to cooperate against any threats towards the alliance. These documents connect the two nations' resources to combat against their main threats like Russia and China. [5]. Japan's government also has a National Security Strategy, which underscores the need for partnership with the U.S. for increased strength and protection in cybersecurity for both countries. They strive to build the foundation of information security by conducting surveillance operations, sharing joint intelligence and facilities, and partaking in bilateral operations;

which include using advanced technological equipment and coordinating counterstrike operations. Further sustaining the partnership with America allows both nations to amplify their security [6].

Germany
Germany and the United States have agreed to several frameworks and policies to enhance technological capabilities and develop robust cybersecurity measures. The 2022 US-EU cyber dialogue highlights an inclusive, collaborative and secure cyberspace [7], and the Budapest convention on cybercrime establishes an international communication system where cyber incidents are reported and shared between participating countries, including the U.S.[8]. Additionally, Germany is one of the countries that endorsed the first global guidelines created by the U.K.'s National Cyber Security Centre (NCSC) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which aids AI developers to make ethical cybersecurity decisions [9]. The establishment of these frameworks and agreements ensures a more resilient cyber ecosystem that demonstrates the maturity of their alliance by showcasing each nation's efforts in safeguarding technology.

Canada
The U.S. and Canada reestablished their cross-border crime forum which has been recently reworked to include cybercrime. The forum emphasizes the necessity to defend against cyber-attacks, encourage cyber hygiene to the public, and the need for collaboration during the Russian-Ukraine war [10]. Furthermore, the Five Eyes (FVEY) alliance was established between the U.K., Canada, Australia, and New Zealand with the purpose of being an intelligence coalition. The FVEY collects and shares signals intelligence, data from communication and information systems, amongst allied nations [40]. In other instances the U.S. and Canada have explored cybersecurity in critical infrastructure such as energy. In 2016, the Joint United States-Canada Electric Grid Security and Resilience Strategies were created by both nations to tackle critical infrastructure concerns and more specifically explored the opportunity to improve the electric grid and eliminate vulnerabilities [11].

Comparative Analysis
Though all these countries may seem to have very similar goals to develop AI, the policies and strategies for each alliance slightly differ. The U.S. and the U.K. alliance is unique compared to the other nations mentioned. The U.K./U.S. alliance has a strong goal to research and ensure the safety of AI. Agreements like the MOU where both nations have invested money and resources into each other for the research and development of AI. Although Germany and the U.K. are located in the same region, their partnership with the U.S. differs. Germany tends to discuss AI and cybersecurity for Europe as a whole while the U.K, Japan, and Canada have several country-specific agreements that allow them to collaborate individually with the U.S..

In addition, the U.K. and Germany collaborate with America through many international initiatives such as the Budapest convention on cybercrime, while Japan and Canada mainly emphasize regional strategies and how to enhance their individual critical infrastructure with AI.

The Utilization of Artificial Intelligence

AI has become a transformative force across the globe and has been revolutionizing sectors and industries within many communities. The diffusion of AI in each country has posed several motivations and concerns regarding the usage of AI. Looking at the similar and contrasting ways of how each country utilizes AI, permits the countries to expand each of their comparative advantages. Using each nation's strengths will allow the allied nations to collaborate more effectively to create a unified force against international threats.

United Kingdom
The United Kingdom plans to become one of the leading nations in terms of Artificial Intelligence by increasing the presence of AI into their society. The U.K's National Cyber Strategy has the intent to protect and promote the U.K.'s involvement in cyberspace. The government allocated $3.3 billion to accomplish the 5 pillars of the strategy: Strengthening the U.K. cyber ecosystem, Building a resilient and prosperous digital U.K., Taking the lead in the technologies vital to cyber power, Advancing U.K. global leadership and influence for a more secure, prosperous and open international order, Detecting, disrupting and deterring our adversaries to enhance U.K. security in and through cyberspace [13].

In addition, the U.K. published the Defense Artificial Intelligence Strategy that envisions transforming the Ministry of Defence (MOD) into the world's most efficient and trusted defense organization for its size. Some main key points in this blueprint is the establishment of the Defense AI Centre (DAIC) and Exercise SPRING STORM. DAIC collaborates with the government, academia, and industries to foster the development of AI in defense, and Exercise SPRING STORM was the first time AI was used in a British Army mission in 2021. An AI-driven engine processed and provided the information of the surrounding environment and terrain during the Exercise [14]. To enact this plan, the U.K. wants to recruit and train talent to evolve their skills for AI, join forces internationally, create clear policies, contribute to the advancement of U.K. companies, and arrange for future leadership and stability in AI through policies [14].

Japan
Japan developed a strategy to address the use and prominence of AI in their society. The government published the Social Principles of Human-Centric AI to base AI regulation on the 3 values of human dignity, diversity and inclusion, and sustainability. Stemming from the three values, the document highlights 7 principles of human-centricity, education/literacy, ensuring security, fair competition, fairness/accountability/transparency, and innovation [15]. With the creation of AI comes the need for regulation, however, Japan acknowledges the concern that too much regulation can harm the innovation and growth of AI. Based on that, Japan has the visions of adopting policies on AI and for AI. While regulation on AI is implemented for the safety and cybersecurity of the nation, regulation for AI promotes the enrichment of AI for the nation [16].

In addition to government plans for policy and regulation, companies and universities have already acted on the progression of integrating AI throughout the nation. Microsoft, an American tech company, invested $2.9 billion into Japan's AI and cloud infrastructure. This large investment aims to train over 3 million people in digital and AI programs. It also enables Japan to have access to more high-end computing resources, allowing for more efficient work and research on AI [17]. Japan's AI ethics are governed by regulatory frameworks that strike a balance between security and innovation [15]. Major IT corporations like NEC and Fujitsu assist Japanese universities, research institutions, and government projects that push improvements in cybersecurity and AI. Japan demonstrates dedication to upholding AI digital security in an evermore complicated cyber environment [18].

Germany
Germany uses AI to combat the creation of malware by implementing sophisticated network security solutions and automated threat detection systems that monitor traffic and prevent illegal access [19]. Germany also investigates hostile AI and malware to comprehend and neutralize such threats [20]. Academic institutions and government programs that encourage the development of cutting-edge AI algorithms and solutions, such as the Federal Office for Information Security and the Fraunhofer Institute for Secure Information Technology, are the main drivers of research and development in Germany [21]. As a result of their proactive attitude, Germany is positioned as a major part in the worldwide endeavor to improve digital security [18].

Mercedes-Benz Group is a German automotive industry that utilizes AI to increase efficiency in manufacturing its vehicles.

Mercedes and Microsoft developed the M0360 Data Platform together, which allows Mercedes' car plants to be connected to the Microsoft Cloud, protecting its supply chain and production resources [22]. Germany has initiatives that aim to educate and increase research in AI like the Cyber Valley. The Cyber Valley is Europe's largest research group in the field of AI and is funded by the Germany Federal State of Baden-Württemberg. Research institutions like this educate the community on AI and also provides opportunities for hands-on experience with AI tools [23].

Canada
Canada's AI framework has grown and appeals to their current and future needs as a country. Canada's investments include an overall $2.4 billion package that will allow for the development of AI [24]. This funding will aid Canada in advancing their deployments and research of AI technologies. The continuous investments that the government of Canada has created for many universities and companies to initiate AI research is promising. This can be seen in the Pan-Canadian Artificial Intelligence Strategy and the National Cybersecurity Consortium (NCC), both funded by the government. The NCC consists of many projects that utilize AI technologies to manage vulnerability, threat detection, then directing systems that mitigate potential threats to 5G networks, along with other AI-based security projects [25]. With the improvement of AI's capabilities, the creation of issues regarding the protection and safety of the nation also grows. Canada has rallied towards enacting codes and acts to strengthen the safety of AI systems [26], such as the Artificial Intelligence and Data Act (AIDA). The AIDA outlines the AI landscapes and frameworks that have been set, along with regulatory procedures in the specific cases of safety concerns or risk management [27].

Comparative Analysis
Each nation acknowledges AI as a focal point for investment into international security However, the contextualization of the AI may vary depending on each country's industries and the principles they prioritize. Each country has different industries that they excel in, resulting in different implementations of AI that would enable them to get the most benefit.

Japan and Canada focus on human-centric AI and balanced regulation, stressing the importance of fostering innovation while ensuring safety and security. Both nations have used AI technologies for the growth of their societies while prioritizing ethical standards. Similarly, the U.K. and Germany emphasize the use of AI in defense and cybersecurity, with the U.K. focusing on specific military applications and Germany on broader security solutions. Canada's NCC and Germany's Cyber Valley are examples of both nations' substantial investments in AI research, displaying advancements through research institutions and academic collaborations. Their global commitment for responsible AI development and utilization are shown through their shared goals and actions.

On the contrary, the U.K emphasizes government-driven initiatives, such as the DAIC to steer AI development, while Japan integrates initiatives from both government and corporate investments, like Microsoft. Japan also ensures that its regulations do not impose excessive constraints, whereas Canada's AIDA heavily stresses the importance of safety and risk management of AI systems. Nonetheless, the U.K. and Germany formulated regulatory measures with a strong focus on international cooperation and the ethical use of AI, assuring that these advancements align with global standards and ethical considerations.

Nation-Sponsored Attacks/Threats

As AI has many different functions to benefit and expand the efficiency of societies, governments are also acknowledging that it can be harmful. Hackers have discovered ways for AI to develop malware, and on a deeper level, use that malware to breach critical infrastructure for countries and industries. By looking at how cyber actors are targeting their allies, the U.S. becomes well-informed, leading to partnerships with allies to fortify against adversaries. Noticing patterns of attacks and how the adversaries operate allow for the U.S. to be one step ahead of incoming threats, which creates and maintains a safe cyber environment internationally.

United Kingdom
The NCSC publicly announced that AI is expected to enhance ransomware and other threats. They claim that ransomware is the most common cyber threat for organizations and businesses, so the U.K. government continues to be cautious of the presence of AI in these cyber attacks [28]. The National Crime Agency (NCA) also conducted research that discovered cyber criminals utilizing Generative AI and offering it as a service for those willing to pay. James Babbage, the Director General for Threats at NCA, concluded that ransomware continues to be a serious threat and will likely spiral due to the evolution of Artificial Intelligence [29] [30].

In 2024, Chinese hackers conducted a cyberattack on the Britain Ministry of Defense, leaking confidential data on the members of the U.K.'s military special forces. The Chinese hackers infiltrated a third-party government contractor to access the names and bank information of current and former employees of the military [31]. The U.S. and U.K. are currently working on ensuring the safe development and usage of AI due to the large sums of cyber attacks.

Japan
According to Kazutaka Nakamizo of Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC), hackers backed by China are increasingly targeting critical infrastructure, with cyber incidents escalating from 150 cases in 2021 to 230 in 2022, with the rise of attacks accumulating [32]. Speaking at the Munich Cyber Security Conference, Nakamizo emphasized the dangers of these threats, pointing out that some attacks have exploited unknown network vulnerabilities. In December 2023, the U.S. sanctioned their own operation to disrupt a "Living of the Land" botnet attack from Volt Typhoon, a Chinese government operation created to disrupt critical infrastructure in other countries [33]. Although this specific attack was disassembled, Volt Typhoon still remains a persistent and priority threat. In September 2023, Chinese hackers were implanting firmware implants in routers to target government agencies, businesses, and industries in both Japan and the States [31]. There have also been recent infringements at Japan's Ministry of Foreign Affairs, the aerospace agency JAXA, and companies such as Yamaha and Seiko, suspectedly caused by Chinese hackers. [32]. Japan continues working with the U.S. to reinforce their cybersecurity and has since increased the staff and budget of NISC to strengthen its response, emphasizing private-public partnerships.

Germany
The ongoing conflict between Russia and Ukraine has caused serious cybersecurity issues in Germany. This battle demonstrated how cyber capabilities may be integrated into traditional warfare, as Russia employed distributed denial-of-service (DDoS) strikes and other cyber operations for propaganda and surveillance [34]. The Russian hacker group APT28 (Fancy Bear) have conducted several cyberattacks on Germany including hacking the Social Democratic Party, defense, aerospace, and IT sectors. The goal of these cyberattacks were to sow doubt and erode confidence in German government agencies to disrupt the peace in the European region. This incident serves as a reminder of Germany's continuous efforts to strengthen cybersecurity defenses, work with foreign allies, and negotiate the challenges posed by AI to counteract evolving cyberthreats. Germany will continue to place a high priority on cybersecurity resilience in order to protect its vital infrastructure and national security from sophisticated, ongoing nation-sponsored cyber attacks [35].

Canada
The Living Off the Land attacks from the Volt Typhoon, deployed by China, caused damage to the infrastructure of the U.S. and allies, including Canada [36]. This has led to a joint agreement between the U.S., Canada, and other allied countries to establish stronger cyber defenses. Additionally, other threats by China were linked to attacks carried out on social media used to spew propaganda about Canadian officials [37]. Similarly, Russia exploited social media algorithms to push a narrative using

augmented images of Canadian forces partaking in war crimes while assisting Ukraine during the Russian-Ukrainian war [38]. These events demonstrate the urgent need for international cooperation and enhanced cybersecurity measures to protect against sponsored cyber threats and attempts of disinformation.

Comparative Analysis

The existence of alliances between countries is to be prepared for any potential threats, which in turn makes it crucial to also look at the adversaries. Adversaries are constantly trying to evolve and create new ways to ambush the U.S. and its allies. By examining previous attacks and potential threats, the U.S. and its allies can distinguish patterns and create stronger methods to safeguard their critical infrastructure.

The incorporation of AI into the creation of malware allows hackers to efficiently develop and employ their attacks. Furthermore, the U.S. and the allied nations mentioned have encountered significant cyber threats from China and Russia. The U.K. and Japan have experienced breaches of sensitive government data by Chinese hackers while Germany and Canada have faced disinformation propaganda efforts employed by Russia. Though all nations have encountered unique cyber threats, they all emphasize the importance of international cooperation to enhance defenses. A persistent threat that all nations examined are the Volt Typhoon attacks conducted by China and ransomware.. The U.S., U.K., and Canada, have all participated in a joint security advisory in order to create a mutual mitigation strategy when potentially facing these Volt Typhoon attacks. Nations have developed strategies and shared resources in efforts to mitigate/prevent similar cyberattacks.

Conclusion & Future Goals

With the continuous progression of AI, the world is slowly revolving around it. The innovations of AI-driven technology have provided communities with numerous benefits but also increases the cyber complications. America and its allies, U.K., Japan, Canada, and Germany, are under constant pressure to maintain cyber defenses against adversaries leveraging AI for malware development and infrastructure deployment.

The future of AI relies on the actions made today. The U.S. and its allies must continue and strengthen collaboration to leverage each country's strengths to enhance cybersecurity and harness the development of AI by sharing knowledge, resources, and practices. As the amount of ransomware threats have been increasing, the U.S. needs to create a unified front with their allies to fortify the digital environment against cyber actors. China and Russia are becoming an increasing threat as they are behind various cyberattacks on various governments' critical infrastructure.

Though adversaries are utilizing AI-driven attacks, the U.S. and its allies can employ AI for cybersecurity methods like autonomous patching, where AI is able to automatically detect and resolve a nation's vulnerabilities and defend against cyber attacks. Having AI as a defensive mechanism increases the efficiency and proficiency of cybersecurity by reducing the amount of time and limiting human error for a sanitized digital ecosystem [39]. To progress in AI defense mechanisms, there is a need for more unity between governments and their specific policies, increased funding or research, and the cohesion between private and public sectors to maximize every opportunity to its full potential.

About the Authors

Brian Lemus is a senior at George Mason University pursuing his undergraduate degree in Information Technology, with a concentration in Cybersecurity. Brian is planning on interning at Apple Federal Credit Union as an IT intern this summer.

Fatima Majid is an undergraduate student at George Mason University, pursuing a degree in cybersecurity engineering. She is interested in cyberlaw and malware analysis.

Bella Nguyen is an undergraduate student pursuing bachelor's degree in management information systems at George Mason University. She is interested in starting her career in networking and security, along with cloud computing. Bella hopes to later become a Project Manager.

Quan Vo is an undergraduate student at George Mason University studying Information Technology with a concentration in Cybersecurity. Quan is interested in network security and is planning on getting his MBA with a concentration in Telecommunications.

Brian K. Ngac, PhD is an Instructional Faculty Member and Dean's Teaching Fellow at George Mason University's Costello College of Business, and a Parsons Fellow. He's the Founding Director of the Professional Readiness Experiential Program (PREP) where Honors and High Performing Students work on real projects with real industry participants to gain hands-on experience prior to their graduation. Any interested organizations that would like to be an industry participant are encouraged to contact bngac@gmu.edu

Nirup Menon, PhD is a Professor of Information Systems and Operations Management in the Costello College of Business. His research interests include information security management, healthcare informatics, and online platforms. He has published over 30 peer-reviewed articles and is serving (and has served) on the editorial boards of leading academic journals in information systems.

References

[1] "What Is Artificial Intelligence? Definition, Uses, and Types," Coursera, Apr. 03, 2024. https://www.coursera.org/articles/what-is-artificial-intelligence?msockid=25c995df49586d85269887b5484a6c5c.

[2] The White House, "The Atlantic Declaration: A Framework for a Twenty-First Century U.S.-UK Economic Partnership," The White House, Jun. 08, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/08/the-atlantic-declaration-a-framework-for-a-twenty-first-century-u-s-uk-economic-partnership/

[3] Department for Science, Innovation and Technology, AI Safety Institute, and The Rt Hon Michelle Donelan, "UK & United States announce partnership on science of AI safety," GOV.UK, Apr. 02, 2024. https://www.gov.uk/government/news/uk-united-states-announce-partnership-on-science-of-ai-safety

[4] W. Henshall, "U.S., U.K. Will Partner to Safety Test AI," TIME, Apr. 01, 2024. https://time.com/6962503/ai-artificial-intelligence-uk-us-safety/

[5] The White House, "Indo-Pacific Strategy of the United States," The White House, Feb. 2022. Available: https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf

[6] National Security Council, "National Security Strategy," Ministry of Foreign Affairs of Japan, Dec. 16, 2022. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf

[7] Office of the Spokesperson - Matthew Miller, "The 2022 U.S.-EU Cyber Dialogue - United States Department of State," United States Department of State, 2022. https://www.state.gov/the-2022-u-s-eu-cyber-dialogue/

[8] Council of Europe, "Budapest Convention and its Protocols," Cybercrime, 2014. https://www.coe.int/en/web/cybercrime/the-budapest-convention

[9] E. Schroeder, S. Scott, and T. Herr, "Victory reimagined: Toward a more cohesive US cyber strategy," Atlantic Council, Jun. 14, 2022. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/victory-reimagined/#alliesandpartners.

[10] "The U.S. and Canada Reestablish the Cross-Border Crime Forum | Homeland Security," www.dhs.gov, Mar. 22, 2022. https://www.dhs.gov/news/2022/03/23/us-and-canada-reestablish-cross-border-crime-forum

[11] Government of the United States and Government of Canada, "JOINT UNITED STATES-CANADA ELECTRIC GRID SECURITY AND RESILIENCE STRATEGY PRODUCT OF THE Governments of the United States and Canada," 2016. Available: https://natural-resources.canada.ca/sites/www.nrcan.gc.ca/files/energy/pdf/JOINT%20GRID%20SECURITY%20AND%20RESILIENCE-Strategy_en.pdf

[12] The White House, "Roadmap for a Renewed U.S.-Canada Partnership," The White House, Feb. 23, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/23/roadmap-for-a-renewed-u-s-canada-partnership/#:~:text=The%20Roadmap%20for%20a%20Renewed%20U.S.-Canada%20Partnership%20announced

[13] HM Government, "National Cyber Strategy," 2022. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

[14] Ministry of Defence, "Defence Artificial Intelligence Strategy," Jun. 2022. Available: https://assets.publishing.service.gov.uk/media/62a7543ee90e070396c9f7d2/Defence_Artificial_Intelligence_Strategy.pdf

[15] Council for Social Principles of Human-centric AI, "Social Principles of Human-Centric AI," Feb. 2019. Available: https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf

[16] H. Habuka, "Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency," www.csis.org, Feb. 2023, Available: https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7-presidency

[17] Microsoft Source, "Microsoft to invest US$2.9 billion in AI and cloud infrastructure in Japan while boosting the nation's skills, research and cybersecurity," Microsoft Stories Asia, Apr. 09, 2024. https://news.microsoft.com/apac/2024/04/10/microsoft-to-invest-us2-9-billion-in-ai-and-cloud-infrastructure-in-japan-while-boosting-the-nations-skills-research-and-cybersecurity/

[18] S. Cesareo, J. White, and A. Mostrous, "The Global Artificial Intelligence Index," Tortoise, Jun. 28, 2023. https://www.tortoisemedia.com/2023/06/28/the-global-artificial-intelligence-index/

[19] Federal Minister of the Interior, Building and Community, "Cyber Security Strategy for Germany," Federal Ministry of the Interior, Building and Community, Sep. 08, 2021. https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html

[20] N. Faeser, "The State of IT Security in Germany in 2023," Federal Office for Information Security, Nov. 02, 2023. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf?__blob=publicationFile&v=6

[21] The White House, "Biden-Harris Administration Announces Key AI Actions 180 Days Following President Biden's Landmark Executive Order," The White House, Apr. 29, 2024. https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/29/biden-harris-administration-announces-key-ai-actions-180-days-following-president-bidens-landmark-executive-order/

[22] Mercedes-Benz Group, "Mercedes-Benz and Microsoft: For efficiency, resilience and sustainability in car production.," Mercedes-Benz Group, Oct. 12, 2022. https://group.mercedes-benz.com/innovation/digitalisation/industry-4-0/mo360-data-platform.html

[23] J. Williams, "Frequently asked questions," cyber-valley.de. https://cyber-valley.de/en/faqs

[24] "Securing Canada's AI advantage," Prime Minister of Canada Justin Trudeau, Apr. 07, 2024. https://www.pm.gc.ca/en/news/news-releases/2024/04/07/securing-canadas-ai

[25] "2023 Funded Projects," National Cybersecurity Consortium. https://ncc-cnc.ca/2023-funded-projects/

[26] Innovation, Science and Economic Development Canada, "Canadian Guardrails for Generative AI – Code of Practice," ised-isde.canada.ca, Aug. 16, 2023. https://ised-isde.canada.ca/site/ised/en/consultation-development-canadian-code-practice-generative-artificial-intelligence-systems/canadian-guardrails-generative-ai-code-practice

[27] Government of Canada, "The Artificial Intelligence and Data Act (AIDA) – Companion document," ised-isde.canada.ca, Jun. 2022. https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

[28] A. Martin, "British intelligence warns AI will cause surge in ransomware volume and impact," therecord.media, Jan. 23, 2024. https://therecord.media/british-intelligence-warns-ai-will-cause-surge-in-ransomware

[29] NCSC, "Global ransomware threat expected to rise with AI, NCSC warns," www.ncsc.gov.uk, Jan. 24, 2024. https://www.ncsc.gov.uk/news/global-ransomware-threat-expected-to-rise-with-ai

[30] National Cyber Security Centre, "The near-term impact of AI on the cyber threat," www.ncsc.gov.uk, Jan. 24, 2024. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

[31] CSIS, "Significant Cyber Incidents | Center for Strategic and International Studies," www.csis.org, 2024. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[32] D. Antoniuk, "Japan sees increased cyberthreats to critical infrastructure, particularly from China," therecord.media, Feb. 16, 2024. https://therecord.media/japan-critical-infrastructure-cyberthreats

[33] Office of Public Affairs, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure | United States Department of Justice," www.justice.gov, Jan. 31, 2024. https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[34] Department of Defense, "Fact Sheet: 2023 DoD Cyber Strategy," 2023. Available: https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF

[35] "Germany accuses Russia of 'intolerable' cyberattack, warns of consequences," Al Jazeera, May 03, 2024. https://www.aljazeera.com/news/2024/5/3/germany-accuses-russia-of-intolerable-cyberattack-warns-of-consequences

[36] National Press Release, "U.S. and International Partners Publish Cybersecurity Advisory on People's Republic of China State-Sponsored Hacking of U.S. Critical Infrastructure | Transportation Security Administration," www.tsa.gov, Feb. 07, 2024. https://www.tsa.gov/news/press/releases/2024/02/07/us-and-international-partners-publish-cybersecurity-advisory-peoples.

[37] C. S. I. Service, "Mission Focused: Confronting the Threat Environment," www.canada.ca, May 07, 2024. https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2023/mission-focused.html#toc16.

[38] C. S. E. Canada, "National Cyber Threat Assessment 2023-2024," Canadian Centre for Cyber Security, Oct. 28, 2022. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024#fig11.

[39] B. Mark et al., "US-Japan: Advancing Cybersecurity and Resiliency in the Age of Uncertainty," 2024. Available: https://pacforum.org/wp-content/uploads/2024/02/EN-Pacific-Forum-Layout-January-2024-Pass-Pages_Feb7-2.pdf

[40] P. S. Canada, "Five-Country Ministerial," www.publicsafety.gc.ca, Sep. 02, 2020. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/fv-cntry-mnstrl-en.aspx