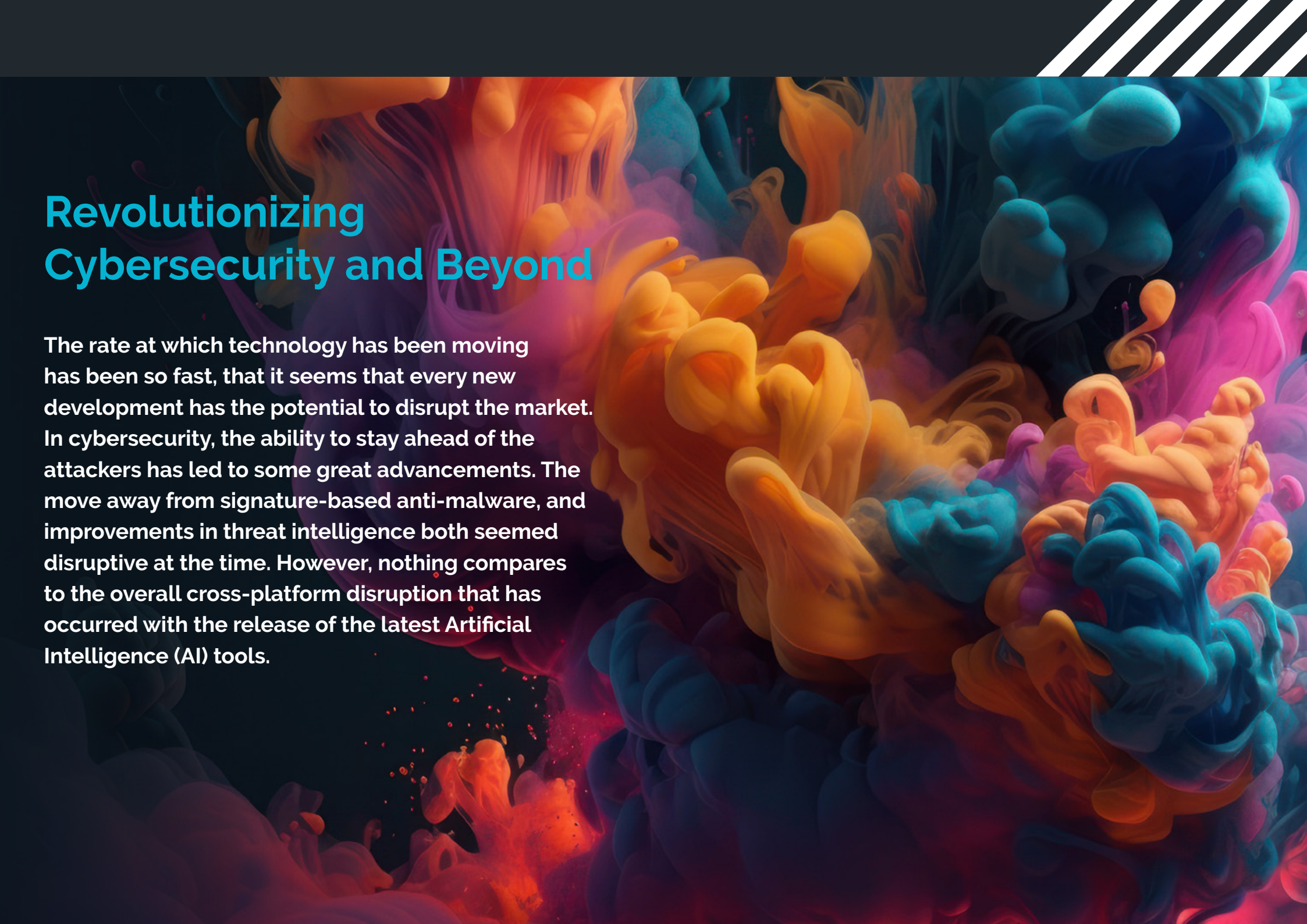




bora

The AI Revolution in Cybersecurity: Transforming the Landscape



Revolutionizing Cybersecurity and Beyond

The rate at which technology has been moving has been so fast, that it seems that every new development has the potential to disrupt the market. In cybersecurity, the ability to stay ahead of the attackers has led to some great advancements. The move away from signature-based anti-malware, and improvements in threat intelligence both seemed disruptive at the time. However, nothing compares to the overall cross-platform disruption that has occurred with the release of the latest Artificial Intelligence (AI) tools.

Artificial intelligence has been with us for a long time. Whether we are seeking information about weather forecasts, listening to a random music playlist, or checking a piece of work for plagiarism, AI has been the method by which these technical marvels operate. Up until this point, our interactions have been very limited. For example, you couldn't ask a weather forecasting application to write a short biography about Socrates or check your programming code for errors. Now, we have been given the ability to directly communicate with AI to generate seemingly free-form answers to many questions.

This disruptive development has resonated throughout all areas of life, from educational systems, corporate meeting rooms and all the way up to governmental discussions about the impacts of AI. What does this all mean to the cybersecurity community? We asked a range of individuals, who occupy a variety of roles related to the cybersecurity industry (from student to CISO) for their perceptions about their uses of AI, and how it may transform the security landscape.



Ravit Jain

Cybersecurity Podcast Host,
Gartner Ambassador, LinkedIn
Instructor, Author

[LinkedIn](#) | [Twitter](#)



Ravit Jain

Cybersecurity Podcast Host, Gartner Ambassador, LinkedIn Instructor, Author

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

Artificial Intelligence has undoubtedly made a significant impact on various aspects of our lives. From enhancing efficiency in industries to transforming customer experiences, AI has opened up new possibilities. As someone who has witnessed the development and application of AI, I find it both exciting and promising. **AI has the potential to revolutionize the way we work, communicate, and solve complex problems. However, it is crucial to approach AI with caution and ethical considerations to ensure it benefits society as a whole.**

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

Yes, AI has become an integral part of my role, especially in the field of marketing. One of the areas where AI has been incredibly useful is in data analysis and predictive modeling. AI algorithms can process vast amounts of data and extract valuable insights, enabling us to make data-driven decisions and optimize marketing strategies. AI-powered tools also help automate repetitive tasks, such as social media scheduling and email campaigns, freeing up time for more strategic initiatives. Additionally, AI-powered chatbots have improved customer service by providing instant and personalized assistance, enhancing the overall customer experience.

The benefits of using AI in marketing are numerous. It allows us to gain deeper insights into consumer behavior, improve targeting and personalization, automate time-consuming tasks, and ultimately increase the efficiency and effectiveness of reaching our target audience.

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

As AI continues to advance, there are several challenges that marketing professionals need to be mindful of. Firstly, ensuring data privacy and security is of utmost importance. With the increased use of AI, vast amounts of personal data are being collected, and it is crucial to handle this data responsibly and transparently. Maintaining ethical standards, including obtaining proper consent and safeguarding data from unauthorized access, will be essential.

Another challenge is the potential bias in AI algorithms. Machine learning models learn from historical data, and if the training data contains biases, the AI system may perpetuate those biases, leading to unfair or discriminatory outcomes. Marketing professionals must actively work towards mitigating

Ravit Jain

Cybersecurity Podcast Host, Gartner Ambassador, LinkedIn Instructor, Author

[LinkedIn](#) | [Twitter](#)

bias in AI algorithms and promoting fairness in their marketing practices.

Moreover, as AI becomes more prevalent, it is important to strike a balance between automation and human touch. **While AI can streamline processes and enhance efficiency, it is crucial to maintain the human element in marketing, especially when it comes to building relationships with customers and understanding nuanced preferences.**

Lastly, the rapid advancement of AI requires continuous learning and adaptation. Marketing professionals need to stay updated with the latest AI developments, understand the limitations and capabilities of AI systems, and adapt their strategies accordingly.

Overall, AI presents tremendous opportunities for marketing professionals, but it is crucial to navigate its challenges responsibly, ethically, and with a human-centric approach.

4). What are some of your favorite AI tools –chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

One of my favorite AI tools is Grammarly, an AI-powered writing assistant. It provides real-time grammar and spelling suggestions, helps improve clarity and conciseness, and even offers genre-specific writing tips. I appreciate Grammarly for its ability to enhance the quality of my written communication, making it more professional and polished.

Canva utilizes AI algorithms to simplify graphic design tasks. It provides a wide range of templates, fonts, and images and suggests design elements based on user preferences.

Chatfuel is an AI chatbot platform that allows businesses to create conversational chatbots for various purposes, such as customer support or lead generation. Its intuitive interface and AI capabilities make it easy to build and deploy chatbots without coding knowledge.

Anastasios Arampatzis

Cybersecurity Copywriter

[LinkedIn](#) | [Twitter](#)



Anastasios Arampatzis

Cybersecurity Copywriter

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

The truth is that there's too much hype (and noise) surrounding AI. It is seen both as a blessing and a curse. AI will solve all our problems, says one side; AI will be our doomsday, says the other. However, as always, the truth lies somewhere in between.

Although AI has many beneficial and life-changing applications, I am mostly concerned that we, as a society, are not ready to embrace this technology in a meaningful and transparent way. Digital literacy is not improving, especially among marginalized and poor communities; countries and societies will be left behind, and inequalities will be amplified. I am concerned that we have learned nothing from the past and will continue to figuratively hit our heads against a wall.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

The use of AI in content writing and marketing is another much-debated topic. **Many say that generative AI tools can be used to improve content; however, I believe there are certain limitations to the extent that these tools can replace human creativity and a personal tone of voice.** My approach to generative AI tools is that they can become perfect assistants in getting content ideas and improving content, especially for non-native English speakers. This is the way that I am using a proofreading tool - to check content for consistency and to improve my writing skills.

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

There are many challenges around AI - cybersecurity and privacy alike. We have already seen reports that AI tools can be used to create malware or craft very convincing phishing emails. Many privacy organizations have also cited concerns about the data that these tools utilize to train themselves. However, **one of the major challenges related to content writing and marketing is the normalization of disinformation.** Since these tools use online content to be educated, disinformation and misinformation can be replicated through AI-generated answers without the user having the ability to fact-check whether the information is true. This issue pertains to the lack of transparency often surrounding these tools, which seem to operate clandestinely.

Konstantinos Kakavoulis

Founding Partner at Digital Law Experts
(DLE), Co-Founder at Homo Digitalis

[LinkedIn](#) | [Twitter](#)



Konstantinos Kakavoulis

Founding Partner at Digital Law Experts (DLE), Co-Founder at Homo Digitalis

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

I firmly believe that it is still too early to assess the impact of ChatGPT and similar platforms in our everyday lives and society. However, the change that they have brought to various aspects of life is astonishing: from playful attempts to create fictional paintings, poems, or songs to the writing of important essays or code, AI tools have gained unprecedented fame.

On the other hand, **we have seen some countries and large, well-reputed legal entities ban or set strict limits on the use of such tools.** Therefore, it is clear that their acceptance is not universal. This is absolutely normal. How can we expect everyone to accept something that almost no one knows how it actually works?

With so much attention being given for the first time in human history to AI tools, we have a unique opportunity: regulate the use of AI in a way that addresses the structural, societal, political, and economic impacts of the use of AI, is future-proof, and prioritizes affected people, the protection of fundamental rights and democratic values. This is the aspiration of the EU AI Act, that we expect to be adopted in 2023.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

It might come as a surprise to most readers, but AI has been used for years in our everyday lives prior to the intrusion of ChatGPT. **I am constantly using AI in my role as a lawyer, a citizen, a consumer, a music lover, a vehicle driver, and a human being.**

Think of some examples that might also apply to you:

- The personalized results we receive when we search for anything on a search engine.

- The best route to follow to avoid congestion with precise timing of arrival when using maps applications.
- The License Plate Recognition cameras that you might have encountered in many parking areas, which automatically recognize your vehicle's license plate.
- The digital phone assistants which recognize our voice instructions used by banks or telecommunication companies.
- Applications that identify the music track we listen to (such as the well-known Shazam).
- The personalized advertisements that are provided to us by websites and social media platforms through online bidding that takes place in less than one second.

We might not always understand it because most of these AI applications have not been promoted to us as "AI-driven services." However, it is an undeniable fact; The use of AI is everywhere.

Konstantinos Kakavoulis

Founding Partner at Digital Law Experts (DLE), Co-Founder at Homo Digitalis

[LinkedIn](#) | [Twitter](#)

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

There are certainly great challenges in the use of AI. I would not confine my response by saying that these challenges are sector or company related. They are horizontal for everyone.

All these challenges must be clearly dealt with by the EU AI Act. To mention only a few:

- Remote Biometric Identification in publicly accessible spaces.
- Predictive policing, discriminatory practices, and undermining the presumption of innocence.
- AI in Migration and border contexts.
- Emotion recognition.
- Biometric Categorization.

- Transparency for the public and for affected persons.
- Accountability for human rights and law violations.
- Rights and redress for persons impacted by AI.

Notably, the lengthy discussions in the EU instruments have led to the EU AI Act currently being shaped, taking into account all, or at least most of, these challenges.

As the saying -which has become famous through Stan Lee's Spiderman, goes: "With great power comes great responsibility." But **AI cannot be held responsible itself, although it possesses great power. So, it is up to us as AI users, but mainly up to the legislators to regulate the use of AI wisely.**

It must be underlined that the regulation of AI in the EU shall be far from enough. The use of AI and its impacts do not have boundaries; they are global. And as such, they should be regulated by global common rules.

4). What are some of your favorite AI tools –chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

I am quite an old-fashioned guy, although relatively young. I have used, and I am currently using, various AI tools to test them or because I have no other choice. I have to admit that maps applications have saved me on various occasions from being late for important meetings or from getting lost.

But really, does using Shazam offer you the same enjoyment as asking the DJ about the great song that was just played at the bar you are in?

Alison Cameron

Cybersecurity Copywriter

[LinkedIn](#)



Alison Cameron

Cybersecurity Copywriter

[LinkedIn](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

The truth is **AI tools are going to be increasingly helpful when it comes to creating SEO-driven content that needs to be a specific length, number of target keywords, and answer a set list of questions.** For instance, I'm working with one client to set up a process where they use an AI tool to craft the SEO article, and then I would fact-check, copyedit, and introduce a more human touch to the piece.

What I do find concerning, however — and I'm sure this is just part of the global learning process of using these tools — is that some companies are letting go of their writers because they feel the tool can do the same work. That's not the case. I think the teams that are going to do best are the ones that leverage AI tools to enable their writers to work faster and better.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

As a writer for B2B tech companies, I see AI as a tool that can help and support me, particularly when it comes to ideation. For me, AI tools like ChatGPT are great for helping me overcome a creative block, making sure I'm addressing the points in a piece that are relevant to the target audience, and sense-checking my approach to an article.

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

I think there's going to be a period of time as companies and writers alike try to figure out how best to use AI. **Today's contract writers are already being asked to edit drafts written by AI rather than write their own original content and reduce their fees, even though they still have to do the work of fact-checking and editing the piece for consistency**

and the like. On the flip side, some brands and publications don't want to publish content written by AI, so they're using tools to check any content that's submitted to them and refusing anything that's found to be generated by AI. The challenge here is that it limits how writers can use AI tools to get the ball rolling on an article.

To me, the next year or so will find more alignment around how AI tools can be best used in the content space, but we're not quite there yet.

Stuart Coulson

InfoSec Consultant

[LinkedIn](#) | [Twitter](#)



Stuart Coulson

InfoSec Consultant

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

It's way too early for us to start making long-term predictions on AI. ChatGPT has only been out for a few months, and yet the hype train is at full speed. For any businesses assessing AI and its potential impact on your business, do your homework, but treat the hype you read very lightly. **As with all new technologies like 3D televisions, there is the potential that this technology may not be right for now and will take time to find its place in businesses.** Think also about the use cases - where will this additional tool add value to your organization? Don't get sucked in by the hype, and invest in something that is a distraction rather than something that will genuinely add ROI. Remember, human creativity will outstrip AI.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

I tried some of the image generators but with little success. I have had more success using ChatGPT for creating ideas for blogs and giving me a launching point for content. However, I have noticed that some of the answers I get are not accurate. As a result, I only use it for ideas rather than using it as a truth. **One area it has become useful, though, is creating speaker bias. I have a hard time promoting myself, so I type something up, and I use ChatGPT to correct the sentences.** One area I would like to see AI improve is workflow automation and for it to contextually understand what I am trying to achieve.

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

We need to control the narrative, not the technology. There needs to be a clear definition of what is AI, what is ML, and what the algorithms are. This will prevent users from being sold an apparently powerful tool which is simply following a rule set. The AI manufacturers also need to disclose the data sources for the answers you receive. This will help users to know where the opinion and bias have

come from in the answers, as well as potentially any disinformation. Unfortunately, the reliance on AI for answers will also reduce the need for critical thinking in decision-making.

In the sphere of cybersecurity, we need to be wary of evidence that is provided by AI sources without critical thinking. We also need to be careful about buying AI systems - check from vendors what algorithms, data sets, and language models are being used.

4). What are some of your favorite AI tools - chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

I have been recently talking to an organization (Left Foot Forward) that is using ReTool, which is low-code. They are using it to automate and reduce the overhead of creating Change Requests, which is the bane of most IT departments! They have also created a tool (GhostPosts.AI) which can help generate social media post ideas aimed at specific age groups and in certain language styles.

Ross Moore

InfoSec Analyst

[LinkedIn](#) | [Twitter](#)



Ross Moore

InfoSec Analyst

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

Any time there's technological disruption, there's accompanying trepidation by many of those affected. ChatGPT is one such disruption, perhaps more keenly felt because communication with words cuts across all industries, and it's open to all; even its advanced features are available for a small charge. Going beyond words to other Generative AI (GenAI) tech, areas such as art, music, video, and application programming are impacted by the changes.

Imperfect designers make imperfect systems, and there are no perfect designers. AI has been around since the mid-1900s. A subset of AI is Machine Learning (ML), followed by Deep Learning, and then by GenAI. **It's important to distinguish what's what when more specific conversations about true AI arise. Much of what's called AI is actually ML, and the newer conversation is generally about GenAI.**

There's a lot of good, and there's a lot of bad, but it's not going away. Individuals and businesses have to

adapt; that kind of forced adaptation is unpleasant, but because there's a lot of good in it, there's a treasure trove of progress to be made.

One potential way to leverage AI is to fill cybersecurity job roles. There's plenty of anecdotal evidence to point to those currently in those jobs being able to do more in less time in their current roles. What if one employee, wisely and professionally using AI, could fill two or more roles? That would immediately reduce the number of open cybersecurity jobs.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

Endpoint protection

The endpoint protection products I use are AI-driven. AI improves attack prevention, as some estimates point out 300,000 new malware pieces are detected each day. Data scientists work with malware samples and attack patterns and trends to create detection models; the more attack methods they sample, the more data they input, ending with improved predictions, detection, and response.

Communications

For various and sundry of my security roles, GenAI has helped draft several responses for various requests. Consequent to the increased velocity of the information gleaned, more information can be

orchestrated, saving tons of time in searching tabs and links for that valuable and relevant point or two.

While it's important to know that one is talking to a computer, using it as an idea generator, and verifying the information presented, it's genuinely fun to have those conversations and discover the capabilities.

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

Ethical use

Have a personal and professional ethos around the use of AI/ML. Why is it used? For what purposes? This delves into different philosophical concepts, mainly centered on "Just because you can, doesn't mean you should."

Take Personally Identifiable Information (PII) as an example. Many people are unconcerned about their personal information being shared, but many other people are concerned. It will take the most restrictive set of controls to ensure regulatory compliance. Businesses should only collect and use what is needed and legal. This principle is in place now, but AI use in a company - especially GenAI - needs to remain vigilant in what data it ingests and how it uses it, e.g., negate the ability to create prompts that are harmful to individuals and businesses.

Ross Moore

InfoSec Analyst

[LinkedIn](#) | [Twitter](#)

Avoid “washing”

In the same vein as ethical use, but different enough to warrant a separate discussion, is avoiding AI washing, which is when companies exaggerate or misrepresent the extent of AI use in their products and services. Creating false perceptions and misleading customers will, at minimum, lead to mistrust and, at worst, harm.

Don't Trust, and Verify (beware of misinformation and hallucinations)

Because it's an imperfect system that's meant to assist but not guide people, AI should be viewed as an assistant that needs verification before making decisions. Like any other tool, it's not one-size-fits-all. As a tool in its infancy, it needs to grow up before we find all it can really do and avoid what it can't be trusted to do.

Improve, not Replace

The future of one's career is knowing how to use AI, but AI shouldn't be used to replace one's personal responsibilities. The world now has

bots to replace the regurgitation of information - professionals need to be able to leverage that speed and add their wisdom and experience to it to demonstrate true, personal value.

It's a tool, and how it's used depends on the ethics of the tool-wielder. Many useful network scanning tools are used by good and bad people. GenAI isn't much different, though it's more powerful because of its ubiquity and accessibility. One description I like about the current state of AI is "Intelligent, but naive."

4). What are some of your favorite AI tools –chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

Art

I use Dall-E to create images for music that I create and upload. I don't make any money off it - it's just a fun thing to do.

Writing

ChatGPT, Copy.ai, Storylab.ai, and Quillbot.com have helped a great deal in generating and exploring new ideas in writing, storytelling, and teaching. Being able to refine prompts and discuss possibilities allows me to create better storylines, characters, outlines, and summaries.

People used to have to go to the library and pore over book volumes for hours to find a few bits of information. Then people could buy their own encyclopedias. Then came more affordable books. Then came the internet and its international resources. AI/ML has created the next iteration. Just like all those other resources, it's incomplete and could stand verification and corroboration before making life-changing decisions. But the speed with which information can be coalesced and distributed is immensely faster. With this velocity increase, it takes much less time to generate ideas and less time to research.

However, with the greater volume of information presented, there's more to research on my end to ensure the veracity of the data - and in the end, I learn a lot more than before. The time it takes to write is about the same, but the quality is better informed.

Information Security

Phind has been useful in tasks such as testing and exploring Python and PowerShell scripts for use in security assessments. I've also started using DorkGPT to better determine attack surfaces and better secure companies.

Anthony M. Freed

Strategic Communications Leader

[LinkedIn](#)



Anthony M. Freed

Strategic Communications Leader

[LinkedIn](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

First of all, it pains me that we keep calling it AI - it's not intelligent. It is just really efficient machine learning. Want to know how we will know when it is intelligent? When it can assess and identify, based on what it already knows, what it does not know, and then what steps to take to synthesize or empirically derive the unknown. This is what humans do - we have a body of knowledge, and then it occurs to us what we don't know, and we form a strategy to fill the gap. **All these current models can do is be really fast and efficient at organizing what it knows, but they cannot synthesize or even understand what it does not know and how to learn it.** As far as what it can do in that limited capacity is an amazing and really powerful tool.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

I have been playing with tools like ChatGPT to quickly and efficiently create outlines that really save me a lot of time in just planning what needs to go into a piece. It does a really good job of giving you the basic structure. What it can't do is actually produce quality content - no amount of querying produces content beyond the depth of a pamphlet, so **writers need not worry yet, unless all they produce is marketing copy an inch deep. It's a tool, a time saver, but it simply can't derive deeper insights required for producing real thought leadership content - it's just a parrot.**

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

People need to remember that these tools grab bits of knowledge from a wide variety of sources

and kind of mash it all together - **there is a big risk to the "real content producers" whose work is being scraped and repurposed** without giving any credit to the person or persons who put in the real work to synthesize new ideas and push our base of knowledge forward. These tools are basically just plagiarizers. If you choose to use them, you need to understand that it is just a helper - you still have to do the work of making the content truly meaningful and impactful, and you have to go back through it all and go find and properly cite the original sources of the information.

4). What are some of your favorite AI tools - chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

I am only using ChatGPT at this point for outlining and getting the basic ideas together, then the research, writing, and citing of sources still takes a considerable amount of time - but as an aid in organizing initial thoughts, it is very powerful.

Ian Thornton- Trump CD

CISO Cyjax

[LinkedIn](#) | [Twitter](#)



Ian Thornton-Trump CD

CISO Cyjax

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

AI has moved more in the public eye, but it is not new. Some aspects are just suddenly becoming the new topic of speculation. There will be a great opportunity for speed improvement and driving efficiency *if* the balance of AI and human checks and balances can be attained. Large Language Models (LLMs) are coming online and becoming available very quickly, but all have limitations based on their training, bias, and scope. We are seeing many inaccuracies in the LLM models where they draw on "the world" to enrich their outputs and confidently regurgitate documents and comments as fact. Decision-making on these dubious facts will inevitably result in inaccurate mitigation or inaccurate assessment of risk.

AI in public view also adds to the amount of pen testing against it, and we have already seen CIA issues with ChatGPT from potential insecurities.

Additionally, my own testing has shown that the model can be tricked into going out of scope, revealing information that a company would not wish to be disclosed and details of its inner OS, as was the case recently with Samsung. It is just a further tool to be used and understood. It does not "understand" its outputs in a deeper meaning of the term or actually care about the product it supplies. It just does what it has been programmed to do. Proper intelligence assessment remains valid and vital in order to turn the information and assessment from the AI into evaluated and assessed intelligence for a SOC to consume.

There are a great many models coming available, some leaked, some with OS licenses, and some that are of unknown origin. As a security vendor, taking these tools as proofed and peer-reviewed is a flawed model, and very few folks out there are actually looking under the hood to understand their new shiny tool.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

Our approach is to use AI algorithms to consider the high-quality data held internally within Cyjax data sources and allow the models to assess correlation and corroboration across that dataset before reporting for our analysts to assess and add value. This approach provides the necessary checks and balances for responsible risk management and accurate intelligence provision. This provides significant efficiency within the processes for the company and drives a more comprehensive approach to intelligence analysis. Additionally, the use of AI provides resilience across the workforce, with some skills being mirrored by the model. This does, however, inevitably mean that the analyst skills had to diversify slightly to understand the new methods of intelligence gathering and risk assessment. **The process of turning information into intelligence remains the same, AI offers the opportunity to move through that process faster.**

Ian Thornton-Trump CD

CISO Cyjax

[LinkedIn](#) | [Twitter](#)

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

As with all new technologies, the challenge is understanding what they can do and what they can't do while holding off the demand to bring AI into the infrastructure to show how cool and advanced the company is. It is reminiscent of the blockchain hysteria, described by some as a solution looking for a problem. The challenge will be remaining calm under pressure and maintaining a good vision of the development cycles with a deeper understanding of the origin, benefits, and risks of various AI algorithms while opening doors to the opportunities available from responsible use. GDPR currently prohibits algorithmic decision-making without human oversight and the processing of personal data without consent, so the inputs into AI need to be compliant. Just because it's new and sexy does not mean the regulatory rules, client confidentiality, and privacy policies are somehow suspended.

I have some deep reservations and concerns about AI, so I'll reserve overall judgment. If it elevates humanity and helps solve global climate change, and supports the advancement and welfare of humans, I am all for it. Unfortunately, judging by how many venture capitalists blew a trillion or more dollars on the Metaverse and now feel that this is the "next big thing", it may become the next cyber gold rush.

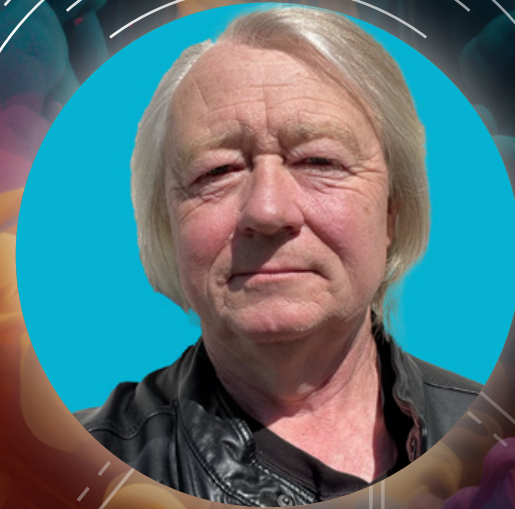
From a cyber security perspective, I am taking a "wait and see" approach, but knowing about Project Mayhem back in 2016, there is a great deal of potential, as we have had seven years of development since these capabilities were publicly revealed, so maybe the benefits of AI and new advances will become tangible as unposed to generally used to amplify cyber security vendor fear, uncertainty, and doubt.

I'll leave you with this one thought I shared at the NCSS in Birmingham: ChatGPT and other AI Large Language Models may solve a huge problem for cybercriminals, providing a single source of all the intellectual property, processes, and services that the organization provides. Now, wouldn't that be a tempting target for ransomware and/or offered for sale on the criminal underground?

Steven Prentice

Cybersecurity Podcast Host

[LinkedIn](#) | [Twitter](#)



Steven Prentice

Cybersecurity Podcast Host

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

AI, in general, and ChatGPT specifically, will continue to have a polarizing effect. Some people will immediately identify the potential for these technologies and will be enthusiastic about their future, while others – most, in fact – will react as they have for all technologies – fearful of what it will do to their jobs and to society. This same reaction has accompanied every major technological innovation and will be dominant until people grow accustomed to it. **The fact that AI is being used in day-to-day activities like smart parking in cars or navigation of intelligent vacuum cleaners shows that we can grow into such developments once exposed to their benefits. A robot is only a robot until it becomes an appliance.**

AI will help take care of much of the work involved in all kinds of jobs, allowing people to focus on the more interesting or lucrative areas. The big fear of not knowing what the truth is with AI-produced information is a serious issue, but we have also been living with that for centuries. Airbrushed/ photoshopped images, propaganda pamphlets, and most recently, social engineering and news networks intent on delivering a partisan message are examples of truth having been manipulated throughout our lifetimes and much earlier. It will be up to individuals to learn to tell the difference.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

As a writer, it would be easy to think that ChatGPT would be a threat to my job. But it's actually a great way to break through writer's block. At this point in time, ChatGPT can generate copy, but it cannot vouch for the accuracy of what it writes, nor can it (yet) assume my style of writing or my understanding of my client's business, needs, message, or voice. It works for me as a writing tool the same way that Microsoft Word's Editor does or even intelligent editors like Grammarly. I also think about people whose primary language is something other than English. Their education and skills have long been held back by a linguistic barrier that they can now breakthrough, opening up employment opportunities and allowing organizations to hire people based on their skill and potential and not exclude them for linguistic reasons.

Steven Prentice

Cybersecurity Podcast Host

[LinkedIn](#) | [Twitter](#)

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

Stage, film, and voice actors need to be aware of being replaced not just by synthetic performances but by illegally obtained copies of their own voices and/or faces. This will require diligence but is still not a unique or new problem. It has been part of the creative media industry for over a century.

With every innovation comes an equal and opposite innovation in the form of a threat (a variation on Newton's third law, perhaps?). Humans are by nature predatory and territorial, and they historically have pounced immediately on new technologies, from metallurgy to software, making them do bad things, while most of the population wants them only for good. Employees, managers, and specialists need to remain constantly aware of the potential for AI technologies to mislead people or

destroy property. This is especially vital in areas such as nuclear deterrence. Perhaps the greatest threat we face is not the source of the information but the speed at which it is sent.

4). What are some of your favorite AI tools –chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

As a writer, I like ChatGPT as a kick-starter and a breaker of writer's block. As a musician, I like AI devices that can separate a recorded song's track to allow me to remove the lead vocalist or guitarist track as a better way to practice (however, I only look for apps that work with artist royalty companies). As a consumer, I look forward to any technology that will replace the message "We are currently experiencing a higher-than-normal call volume" with "Hi, I can help you with that."

Mosopefoluwa Amao

Cybersecurity Student

[LinkedIn](#)



Mosopefoluwa Amao

Cybersecurity Student

[LinkedIn](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

AI benefits people and organizations who know how to use them optimally. AI functionality has increased with the release of tools like ChatGPT and others. AI is here to stay, and while it is exciting to use these tools that help increase efficiency and productivity, it is still volatile and developing, just like every other technology out there.

From a cybersecurity point of view, AI tools pose specific security threats and risks that users ignore. The likes of ChatGPT, which developers are constantly updating, are prone to errors and may produce inaccurate results; therefore, relying solely on these tools can be dangerous. While it is helpful to use these tools, it is essential to carry out due diligence and ensure the produced results are accurate.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

I currently use AI to schedule tasks, plan my days, paraphrase writings, carry out quick research (which I verify), and even plan my meals. AI has been beneficial in ensuring that I complete tasks when due. AI tools like Grammarly have helped my writing by helping me sound better when giving speeches and writing articles. Using tools like Copyscape has helped me scan my writing for plagiarism, and ChatGPT has helped point out details I could have missed while working in my role. Ultimately, the benefits of AI are tremendous if applied appropriately.

Mosopefoluwa Amao

Cybersecurity Student

[LinkedIn](#)

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

In cybersecurity, AI is increasingly used to detect and respond to cyber threats, analyze large data sets for threats, and automate tasks. Despite these fantastic benefits, AI poses several challenges and risks. As a rule, do not disclose personal information to any AI tool you use. AI works with data, data that, if accessed, threat actors can use in the case of a breach.

Threat actors can use AI to develop advanced cyber threats. It can generate phishing emails, deploy malware, or even create fake videos to lure unsuspecting targets. Cybersecurity students should remain current with the latest developments in AI to leverage its benefits and protect themselves and the organizations for whom they work.

4). What are some of your favorite AI tools –chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

My favorite AI tools are ChatGPT, Grammarly, QuillBot, Copyscape, and Canva. I like these tools because of the level of efficiency they avail me. With ChatGPT, I can get answers to any question, provided the data has been updated in its database. With QuillBot, I can paraphrase and rewrite paragraphs; with Grammarly, my writing is arranged in the tone and delivery I intend.

Martina Dove

Senior User Experience Researcher

[LinkedIn](#) | [Twitter](#)



Martina Dove

Senior User Experience Researcher

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

I think AI is the future, there is so much that it can do for us, and it is certainly getting better. There are some excellent tools out there already that utilize generative AI successfully. But I don't think it can be applied to absolutely everything with equal success. **I am afraid that, with many companies jumping on the bandwagon, there will be products or services that will disadvantage or harm specific groups of people. For example, in the early days of applicant tracking software, algorithms would prioritize resumes based on gender stereotypes.** We have to remember that any AI is as good as the training data it receives. But as humans, we trust technology, assuming that it's impartial and accurate when in reality, it can be neither. We need to make sure to also focus on the limitations that such technology brings and not lose sight that what is easier and more efficient is not always better.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

Not directly related to my role, but **I have wondered about new AI-powered tools that help with research analysis. I am not yet convinced that this is an area where AI can do great things because humans are so complex.** Some of the research tools have experimented with adding AI-powered features. So far, most of the attempts, such as analyzing sentiment in people's feedback or answers, have been hit and miss because people have different ways of speaking, use different words, and often contradict themselves when speaking. They may say something negative but contradict that with something positive. This type of thing is

hard for AI to analyze accurately, so it may just pick either negative or positive aspects. It takes human skills to understand the nuance and assign sentiment to what people are saying. There is so much that comes into it, cultural and social norms and ways of speaking, personality, eloquence, etc. Additionally, a good research analysis is often something that accounts for what is unsaid but implied, something that is causing anxiety or fear. Something intangible that appears through discourse. Those are the interesting insights, not merely describing data in some way but pulling it all in and connecting the dots to create higher insights. I have always been curious about speeding up the analysis but have never found high accuracy with research tools powered by AI. This may change in the future with generative AI, but time will tell.

Martina Dove

Senior User Experience Researcher

[LinkedIn](#) | [Twitter](#)

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

Social engineering and cybersecurity. Fraud is already a huge problem, with cybercriminals getting better and better at creating convincing social engineering attacks. And now, with generative AI, such attacks will become even more convincing and sophisticated, and easy to execute. High-quality phishing emails will become a norm, and it will be hard to tell them apart from reality. Another one is cloning people's voices and creating even more sophisticated deep fakes, including videos. Some of it is already happening, with scams that use voice cloning to convince family members to send money. With generative AI, this is now easier to do, and we will see a lot of harm come out of it as this technology starts to get used more and more by cyber criminals and the general population. I think this will greatly erode the trust we need, as humans,

to conduct business, form relationships, and generally enjoy life. It will be harder to tell fake news from real news, harder to date or form friendships online and know what and who is real. But **I think the biggest challenge will be controlling fraud, which is already an epidemic. Businesses will also have to adapt to not rely on biometrics alone as a way of securing people's data or finances.**

4). What are some of your favorite AI tools –chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

New Relic, the company I work for, has just released GROK - AI powered assistant which helps with observability tasks. It is pretty cool. Observability can be complex, and often, observability products come with their own query languages, which are not always easy to learn. GROK can translate simple questions to queries; it can guide you through data

and get answers to questions you might have, set up alerts, suggest how to fix problems, and more. It's very cool, and I can see it being used a lot by observability professionals, who are often strapped for time.

Kaitlin Harvey

Digital Content Manager

[LinkedIn](#)



Kaitlin Harvey

Digital Content Manager

[LinkedIn](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

A lot of people have a negative perspective on this topic, but I'm cautiously excited to learn more about it. AI is just a tool, and—at least with what I've explored so far—it's only as effective as the inputs you give it. We're only just starting to see the potential AI can bring to human creativity, and I'll be curious to see how different the AI landscape looks a year from now.

As it stands today, it's no replacement for actual human creativity because only humans can explore truly tangential, off-the-cuff avenues, but AI does work well to help organize thoughts, provide topics and starter content, and helps to just get something, anything, on the page. For instance, if you're facing a tight deadline or being mocked by a

blinking cursor, getting started can be the hardest thing to do. AI can help you simply slide writer's block aside and get the creative gears turning again—and do it in no time flat.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

I have started exploring AI in my daily work as a cybersecurity copywriter. It helps me save time in many areas, including brainstorming lists of potential headlines, simplifying and condensing complex verbiage, summarizing articles, providing outlines, reformatting content types, and even drafting some starter content. There are numerous possibilities, and I know I've only tapped into a sliver of it all. I'm still exploring and learning—and will be for the foreseeable future. Regardless, I edit everything the AI generates because that content is never 100% ready. Often far from it.

AI does make the overall content creation process easier. Since it can summarize my often-messy initial notes and outlines and sometimes create usable, albeit rough, working drafts.

All in all, AI helps me save time and energy so I can focus on more of the types of work I enjoy the most.

3). Moving forward, what will be some of the challenges around using AI? What do cybersecurity and marketing professionals need to be wary of concerning privacy?

One of the challenges I see is differentiation. With the open availability of AI tools, marketing is at risk of becoming a sea of sameness. Granted, two humans aren't going to prompt a tool the exact same way, but the content could start sounding hollow and unempathetic. Human perspectives and creativity are going to be important to ensuring brands aren't lost amidst the noise.

Kaitlin Harvey

Digital Content Manager

[LinkedIn](#)

Biases and misinformation are two other big issues. These tools aren't perfect. They hallucinate—some more than others—and the internet is already rife with misinformation. AI tools could make it even more difficult to discern fact from fiction.

There are also cybersecurity ramifications. Everyone needs to exercise common sense when prompting AI tools because that prompt data gets ingested into the AI's training model and could be used across other conversations with other users. People definitely need to use caution when working with sensitive data or proprietary information.

The content marketing community has a choice to make. I don't think that AI is coming for our jobs, but it will restructure some content creation workflows. I see this as a good thing, and it is exciting, but it's up to us as writers and creatives to upskill ourselves and learn how to tap into these tools to stay ahead of the competition, both on individual and business levels.

The way I see it, the most powerful creatives of the future will be human marketers with machine sidekicks.

4). What are some of your favorite AI tools –chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

ChatGPT and Wordtune are a couple of tools I've explored for writing. With ChatGPT, I love seeing the variation in answers you can get based on how you prompt the tool. I recently got access to ChatGPT4, and I'm excited to see the differences between versions.

Wordtune is cool, too. I can write in one tone of voice and easily recreate it in another with just a couple of clicks. The free version is fairly limiting, but it's still interesting, and the Chrome extension is helpful.

David Corlette

Vice President Of Product
Management

[LinkedIn](#) | [Twitter](#)



David Corlette

Vice President Of Product Management

[LinkedIn](#) | [Twitter](#)

1). With the rise of ChatGPT, we have seen Artificial Intelligence move very much into the public eye. Based on your own experiences with AI, what are your general thoughts on it?

It's important to recognize that AI does not create; it merely regurgitates based on some amalgam of past patterns it has analyzed. We've seen this in popular culture in some of the ridiculous answers it has generated - patently false but based on lots of false content that it previously consumed. In my own area, we use AI to detect new forms of malware using probabilistic matching - which it is great at, but it tends to be less accurate in detecting previously known malware when compared to yes/no signature-based matching.

2). Are you using AI for anything related to your role? If so, what are you using AI for, and what are the benefits?

We use AI to detect malware, specifically previously unknown malware. It's very useful for that use case but worse at catching well-known

malware patterns. Generally, signature detection is much more explicit and accurate, whereas AI is... Just a guess, so to speak, which appears to be correct but has errors: fine for new kinds of malware that signatures wouldn't detect, but definitely less accurate than a hybrid engine could be.

3). Moving forward, what are going to be some of the challenges around using AI? What do content marketing professionals need to be wary of?

It's important to note that AI is just a method; it all depends on how that method is implemented. ChatGPT isn't cool because it's AI; it's cool because its owners spent years training and tuning it on nearly all the content available on the internet. In the malware world, AI isn't useful unless it's well-designed to incorporate data on the right signals and unless it's well-trained on the billions of known malware samples - something new AV vendors don't have access to. **The problem is that consumers have no idea how to evaluate a vendor's claims or to rate the actual real accuracy of a given engine.**

4. What are some of your favorite AI tools - it could be chatbots, AI-generated images, or writing tools? Tell us in 50-100 words why you like them so much.

I've been impressed by ChatGPT, but really, I think all the existing tools are terrible. Although it's really impressive that you can ask ChatGPT about almost any topic, it doesn't take long before you discover that its answers are pretty shallow and really need to be edited and fact-checked before they are usable. At this stage, AI is more like a good search engine, with the ability to merge responses into a single answer - but not much more than that.



Conclusion

AI is clearly a disruptive technology with the power to transform the way we live and work. One thing that becomes clear from the responses of the experts is that, although the technology can influence the future, it is still too early to tell exactly how transformative it can be.

The current newsworthy fears about the destructive capabilities of AI are similar to what was predicted at the start of the industrial revolution, as well as the start of the computer revolution, and robotics. For now, however, the cybersecurity community seems to greet this new technology with guarded optimism.

bora