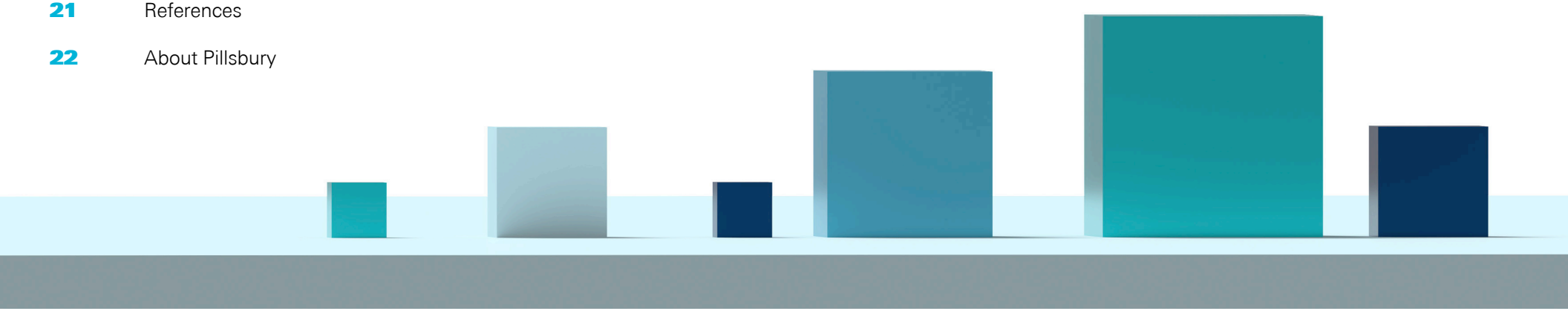
pillsbury

Balancing Innovation,
Execution and Risk

ARTIFICIAL INTELLIGENCE & CYBERSECURITY

CONTENTS



ABOUT THIS REPORT

Artificial Intelligence & Cybersecurity: Balancing Innovation, Execution and Risk is a report from The Economist Intelligence Unit, sponsored by Pillsbury Winthrop Shaw Pittman LLP. Through comprehensive desk research, literature reviews and expert interviews, the report explores the opportunities and challenges of artificial intelligence (AI) as it relates to cybersecurity. Specifically, this report explores the issue from two angles: how AI can help strengthen security by, for example, detecting fraudulent behavior more easily than human watch dogs can; and how the growing need for data to train AI systems is intensifying concerns around privacy and what companies need to watch out for.

We would like to thank the following experts for their time and insights:

- AJ Abdallat, CEO, Beyond Limits
- Johan Gerber, executive vice president of Security & Cyber Innovation, MasterCard
- Ansgar Koene, Global AI Ethics & Regulatory Leader, EY
- Jessica Newman, program lead, AI Security Initiative, UC Berkeley
- Marietje Schaake, president, CyberPeace Institute and international policy director, Cyber Policy Center, Stanford University
- Leo Simonovich, vice president & global head of industrial cyber and digital security, Siemens Energy
- Monique Shivanandan, CISO, HSBC

This report was produced by a team of EIU researchers, writers, editors and designers, including:

- Michael Paterra—project manager
- Kim Andreasson—author
- Michael Gold—editorial advisor
- Amanda Simms—editor
- NWC Design—graphic designer

3D illustrations courtesy of Pillsbury Winthrop Shaw Pittman LLP.

The EIU bears sole responsibility for the content of this report. The findings and views expressed herein do not necessarily reflect the views of our sponsor, partners and interviewed experts.

For any enquiries about the report, please contact:

Michael Paterra
Manager, Policy and Thought Leadership
The Economist Intelligence Unit
New York, United States
E: michaelpaterra@eiu.com

FOREWORD

pillsbury

The frequency and scale of cyber incidents and data breaches have grown exponentially, and in short order. As the public and private sectors have fully embraced digital transformation—a transition only further accelerated by the pandemic-induced shift to remote working—and bad actors have become more sophisticated in their tactics, vulnerabilities to cyber threats have likewise expanded, providing online malefactors new pathways to exploit. The numbers bear this out: In a 2020 analysis, Accenture found that business email compromise events increased year-over-year by more than 50%, ransomware attacks by 160%, and third-party and supply chain intrusions almost tripled.

But artificial intelligence (AI) tools can play an important role in alleviating this growing exposure. These emerging technologies are well-suited to address some of the largest gaps in existing cyber defenses, providing 24-7 system monitoring, streamlining threat detection efforts and independently improving efficacy over time. They can offer layers of organizational data protection not previously available, mitigating human error and ensuring compliance with established cybersecurity policies.

By no means is deploying AI to enhance cybersecurity efforts without challenges, however. Despite its tremendous promise, implementing AI in a cyber context presents risks of its own. Variance in human understanding of these highly complex technologies and their algorithms, a general lack of regulation or established best practices, inconsistent application between (and even within) organizations and increasing use of AI by hackers for their own nefarious purposes all invite new means of manipulating and corrupting data.

But while AI by itself may not be a cure-all for cyber risk, it does have the potential to meaningfully enhance existing cybersecurity and data protection programs in important ways. Utilized concurrently with established human-led information security teams, the two can play off one another's strengths, bringing levels of rigor, vigilance and responsiveness to cyber defense efforts that neither could achieve independently.

In integrating AI technologies with cybersecurity programs and systems, businesses across sectors have an invaluable opportunity to address one of the most complicated and potentially damaging risk factors organizations face today. We hope this report helps illuminate the important role AI stands to play in defending against cyberattacks and data leaks and that the evolution of these promising tools can be deployed to better protect both organizations and the individuals they serve.

Rafi Azim-Khan

Partner, Cybersecurity, Data Protection & Privacy practice co-leader

Pillsbury Winthrop Shaw Pittman LLP

Brian Finch

Partner, Cybersecurity, Data Protection & Privacy practice co-leader

Pillsbury Winthrop Shaw Pittman LLP

Aaron Oser

Partner, Global Sourcing and Tech Transactions leader

Pillsbury Winthrop Shaw Pittman LLP

David Stanton

Partner, Information Law & eDiscovery co-leader

Pillsbury Winthrop Shaw Pittman LLP

EXECUTIVE SUMMARY

The COVID-19 pandemic has accelerated digital transformation across industries, creating newfound benefits to efficiency but also exposing new risks to organizational networks as technology adoption rises and employees increasingly work remotely. As a result, there has been a rapid uptick in the number of cyberattacks, ranging from mundane efforts to gather important business and personal information to highly sophisticated attacks on critical infrastructure. At the same time, the rise of artificial intelligence (AI) across industries provides both an opportunity and a challenge to organizations as they look to leverage technologies to improve their cyber defenses. If adopted and monitored properly, AI can serve as a key competitive differentiator in the success of cybersecurity programs.

This report explores perceptions around the intersection of AI and cybersecurity. It finds that organizations are aware of the opportunities in this regard but also of the potential negative consequences of being overly reliant on AI to protect themselves. The key findings are:

AI can enhance cybersecurity. It primarily does this by automating threat detection by handling substantial volumes and identifying anomalies around the clock, even as human support continues to play an important role. A hybrid approach may provide the best of both worlds; however, control of organizational AI cybersecurity systems should only be provided to a few highly trusted people.

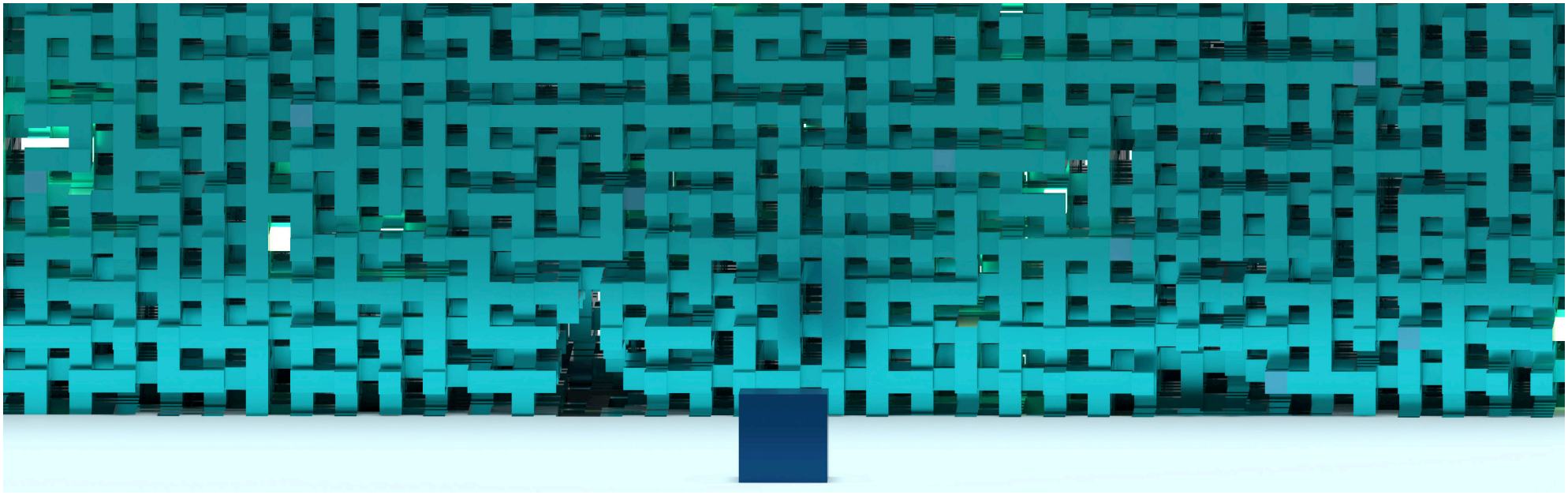
AI can introduce cybersecurity weaknesses. Despite its many benefits, AI solutions are not a silver bullet as organizational governance and policies continue to play a key role in beefing up cybersecurity. In part this is due to the fact that there is a nascent but potentially growing threat landscape in which malicious actors use AI to penetrate weak systems or exploit the complexities of cybersecurity systems that rely on AI.

Regulatory compliance comes to the forefront. Data privacy and transparency are no longer buzz words as companies need to comply with extensive regulations and build trust among customers, regulators and the public. This can pose a compliance challenge for US-based companies due to varying rules across states and the need to adopt international practices if operating in a region such as Europe.

There is hope that an international consensus on AI principles will also lead to global cybersecurity agreements. The lack of common norms and principles related to cybersecurity has long been a sticking point for global agreements. AI may change that too, as the G20 have adopted shared principles on the use of the technology, a nascent effort that may pave the way for further agreements.

CHAPTER 1

A NEW CYBERSECURITY PARADIGM



A confluence of factors has highlighted the importance of cybersecurity. First, cyberattacks are on the rise, particularly in light of COVID-19. People are working from home more and more, a backdrop against which cybercriminals exploit weaknesses. Research from the International Criminal Police Organisation (INTERPOL), a global inter-governmental group, shows that the number of cyberattacks has increased during the COVID-19 pandemic, with major corporations, governments and critical infrastructure frequently targeted.[1] IBM estimates that the average cost of a data breach reached US$3.86m in 2020.[2]

Companies rely on data and technologies even more as they seek competitive advantages, while cyberattacks are becoming more sophisticated and targeting higher-value organizations and their data. To take one recent example, hackers compromised software solutions from SolarWinds, an IT company, allowing attackers to reach multiple high-profile entities, including the US government.[3] The case highlights the importance of the "weakest link" in the cybersecurity ecosystem in which an attack on one company can have a ripple effect on other network systems.[4]

Enter AI, which holds great promise as a means to deal with the complexities of modern cybersecurity challenges. In a recent EIU survey, nearly half of respondents cited AI and machine learning (ML) (48.9%) as the emerging technologies that would be best deployed to counter nation-state cyberattacks directed toward private organizations, followed by cloud computing (47.5%), which is also often touted as bringing enhanced cybersecurity (Figure 1).[5] The Compound Annual Growth Rate (CAGR) for AI in cybersecurity is also predicted to increase at a rate of 23.6% from 2020 to 2027, reaching a market value of US$46.3bn by 2027.[6]

Leveraging existing and emerging threat intelligence, AI can automate incident detection. "AI can basically process large numbers of data files all at once, which is obviously a lot faster than a human could and that really is important," says AJ Abdallat, CEO of AI solutions company Beyond Limits. "The other key thing is that it works 24/7 because AI doesn't need a lunch-break—it doesn't get tired." The continuous monitoring that AI provides is therefore one of its main advantages, along with the fact that it can extract and monitor any minute hitches in the system to flag anomalies. A recent survey of 4,500 senior business decision-makers shows that data security was the main reason to implement AI within their organizations, ahead of process automation and business process optimization, among other areas.[7]

"AI is the only way you can really solve those big complex data problems," says Johan Gerber, executive vice president of Security & Cyber Innovation at MasterCard. This in turn illustrates new challenges for organizations, including the convergence and importance of technology and government regulations such as the revised Coordinated Plan on AI in Europe, which have a growing impact on companies. "If the revised Coordinated Plan on AI is the strongest relevant regulation across the world [then] that's the norm we like to use across everything we do everywhere, so there is integrity in the system," continues Mr. Gerber.

"AI can support the goals of cybersecurity—for example by generating new insights about the behaviors of cyber criminals—but it also exposes us to new vulnerabilities, both because of weaknesses of AI systems themselves, and because of how AI can be used for problematic ends," says Jessica Newman, research fellow at the UC Berkeley Center for Long-Term Cybersecurity, where she leads the AI Security Initiative. AI can therefore serve to strengthen and weaken security simultaneously, depending on whether it is used as an offensive or defensive tool. "Hackers also have access to AI and can use its abilities in order to generate attacks," explains Ansgar Koene, the global AI ethics and regulatory leader at EY.

PERSPECTIVE: THE VALUE OF CYBER RISK RATINGS

pillsbury

Corporate supply chains, vendor management issues, data sharing arrangements and channel partnerships are examples of corporate interdependencies which expose an organization to cyber risks based on how well its counterparts maintain their security infrastructures. Interesting emerging technologies in the marketplace are leveraging AI to address the problem, and seeking to quantify this exposure through corporate cyber risk ratings, analogous to the credit rating score for an individual or organization.

Service providers offering these cyber ratings crawl the internet to continuously monitor the outward facing digital network footprint of target organizations to detect and measure their external attack surfaces. Based on publicly available information, they discern areas of vulnerability and potential exposure to external threat actors. The resulting ratings are derived from the available inputs and applicable algorithms. They can be used by organizations (and their insurers) to evaluate the company's cybersecurity posture, and provide a relatively objective metric that its counterparts can turn to when considering collaborations, acquisitions, and in managing ongoing relationships.

Cybersecurity risk ratings present assessments based on the apparent exposure from an organization's domains, devices and data visible to the internet—often primary entry points for nefarious actors. The ratings illuminate areas where an organization could improve its security hygiene by exposing technology shortcomings (e.g., lack of current updates, bug fixes, patches, outmoded systems, and other vulnerabilities), which are often correlated with human action breakdowns in security management. Recent guidance from the U.S. Cybersecurity and Infrastructure Security Agency noted the role of cyber risk metrics, and characterized such rankings as a "starting point for companies' cybersecurity capabilities and [a tool to] help elevate cyber risk to board-level decision making."

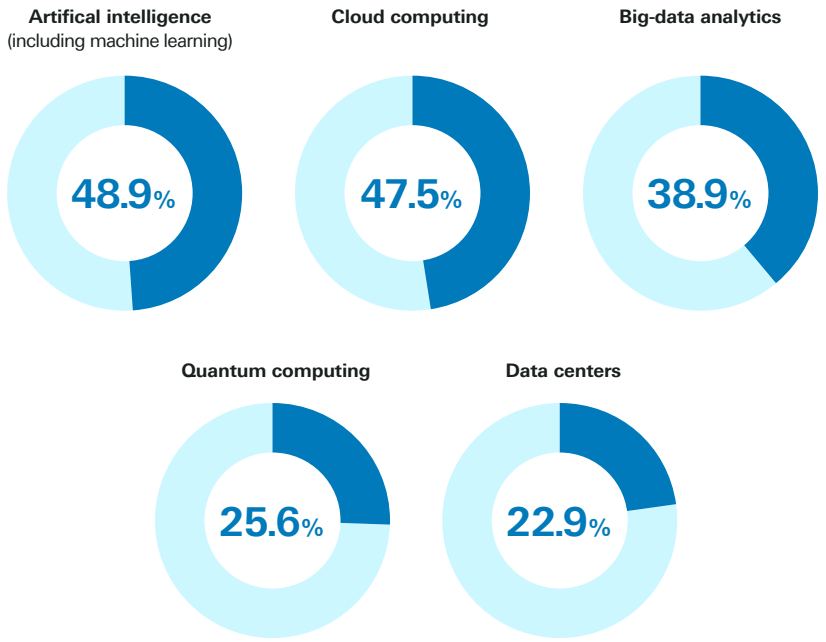
David Stanton
leader of Pillsbury's Information Law & Electronic Discovery practice

See B. Kolasky, "A Risk-Based Approach To National Cybersecurity", January 14, 2021.

Figure 1

Nearly half of executives in Asia-Pacific, Europe, and the United States think AI/ML is the best tool to counter nation-state cyberattacks

Which of the following emerging technologies do you think would be best deployed to counter nation-state cyberattacks over the next five years? (can select more than one)



Source: EIU (2021)

AI exposes new complexities, vulnerabilities

There are three primary areas in which AI presents a cybersecurity risk, according to Ms. Newman. First, introducing AI can add complexity and opacity to the products, services, and infrastructure we rely upon. "There's a shocking lack of industry best practices or regulations to ensure that those AI systems are actually reliable, robust, transparent and free of bias," she says. "We are increasing the complexity of a good portion of the systems that we rely upon across industries, without adequate insight into how those AI systems are making decisions and whether they should be trusted."

Second, there are unique vulnerabilities and safety considerations. "AI technologies are currently susceptible to adversarial attacks, such as data poisoning and input attacks," explains Ms. Newman. "Moreover, AI systems are designed typically to optimize for a particular goal or reward function, yet, the ways in which they end up achieving that goal may be problematic or unsafe."

Third, AI technologies are enabling mass creation of synthetic media. "AI can support the creation of disinformation through large language models that predict text," continues Ms. Newman. "If you imagine that there would be AI-generated language which can use a whole bunch of data to tweak and basically generate a very credible, relevant piece of text, it may also make it easier to trick people into believing that this is actually a true email," adds Marietje Schaake, president, CyberPeace Institute and international policy director, Cyber Policy Center, Stanford University, about the potential pitfalls.

The combination of added complexity to systems by introducing AI, the fact that AI itself is susceptible to attacks, and that adversaries can use AI to create more sophisticated attacks, illustrates that the challenges are as tall as the opportunities when it comes to cybersecurity.

"AI is already being used by criminals in order to overcome some of the world's cybersecurity measures," warns Mr. Gerber. "But AI has to be part of our future, of how we attack and address cybersecurity."

> "AI is already being used by criminals in order to overcome some of the world's cybersecurity measures... but AI has to be part of our future, of how we attack and address cybersecurity."
>
> **Johan Gerber**
> Executive vice president of Security & Cyber Innovation, MasterCard

Defining AI

Artificial intelligence (AI), machine learning (ML), deep learning, and other such terms are sometimes used interchangeably but there are differences.[8] ML is the application of algorithms which underpin AI whereas deep learning is an approach to ML. Hence they are all interrelated and this report uses AI as an umbrella term for all of them to identify their role in cybersecurity.

AI systems are, in general, marked by their adaptability and the recursive way in which they interpret results and modulate future actions based on input. It's a nascent but rapidly emerging area in cybersecurity as implementation models are evolving. For example, cognitive computing systems, a type of AI used to simulate human thought, combines ML algorithms and deep-learning techniques to learn on their own in order to predict cyberthreats.

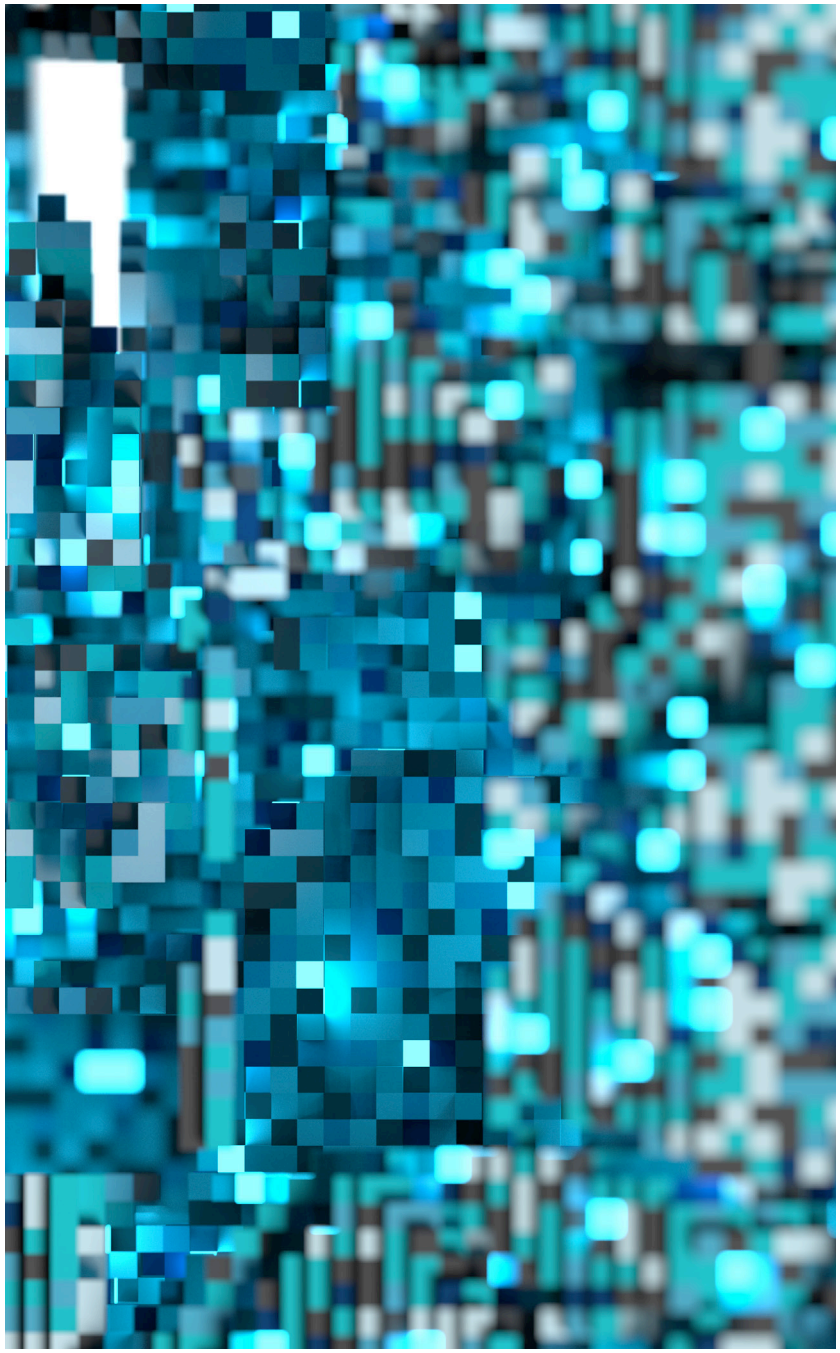
"It's amazing what AI and machine learning can do as they can identify behaviors, patterns and anomalies," explains AJ Abdallat, CEO of Beyond Limits, an AI solutions company. "Based on behaviors and insights, AI and ML allows us to predict something will happen before it actually does," adds Monique Shivanandan, CISO at HSBC, a global bank. "It allows us to take the noise away and focus on the real issues that are happening and correlate data at a pace and at a speed that was unheard of even a few years ago."

CHAPTER 2

AI & THE GLOBAL SECURITY IMPERATIVE

"What we need to do is to be ahead of the bad guys. We have the ability to evaluate a massive amount of data at lightning speed, so we can detect and quickly respond to anything that may happen."

Monique Shivanandan
CISO, HSBC



"However, there's two sides of the coin, because threat actors are also using AI and ML tools," says Ms. Shivanandan. "What we need to do is to be ahead of the bad guys. We have the ability to evaluate a massive amount of data at lightning speed, so we can detect and quickly respond to anything that may happen." However, organizations implementing AI for cybersecurity purposes may also be more vulnerable as they introduce complex systems behind the firewall, unless they understand them. "There are more pathways open to attackers to infiltrate systems and gain access," says Ms. Newman, who also points out that we are likely to see more types of AI-enabled cyberattacks in the future.

To counter all forms of cyberattacks by raising information awareness and improving coordination, countries have long relied on Computer Emergency Readiness Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) to track information about cyberattacks. Recently, the European Union Agency for Cybersecurity (ENISA) has also highlighted the importance of strengthening the cybersecurity ecosystem for AI, indicating the role it has to play in the future.[10] A key part of the ecosystem is related to the need for AI education. According to the AI Index Report from Stanford University, 65% of graduating North American PhDs in AI went into industry in 2019, up from 44% a decade earlier, highlighting the increasing role of commercial AI development—although demand still far exceeds supply.[11] "There is a shortage of talent," says Mr. Gerber. "Organizations are scrambling to get the talent they need at all levels that can monitor the risks as well as do technical implementation," adds Ms. Newman. At HSBC, Ms. Shivanandan agrees that finding the right talent is a key to success. "It's not just about building models but maintaining, growing, evolving, and understanding them to avoid bias or other risks."

Building international consensus

In addition to a talent shortage, there has been a glaring lack of global agreements on cybersecurity and cybercrime generally. Emerging technologies such as AI are often an afterthought in such discussions, despite their growing importance often on display in the corporate world. "New services that pop up show how much more advanced the private sector is when it comes to setting norms before any legislature or other official democratic body has had the chance to," notes Ms. Schaake.

It is therefore necessary for global leaders to finally come to an agreement on worldwide standards in this area. In 2019, the G20 Leaders welcomed a set of AI Principles, based on recommendations from the OECD.[12] The principles seek to foster trust and confidence in AI by promoting inclusiveness, human-centricity, transparency and accountability, among other things. "It's a fantastic starting point to build on, providing a shared language and common set of goals," says Ms. Newman. "But obviously, the principles are just the beginning as we hope to see more accountability for actually holding actors to those standards and principles. In April 2021, the European Commission also unveiled the first-ever legal framework on AI, which addresses the risks of various uses while aiming to promote innovation in the field.[13]

The prospect for international agreements related to AI and by extension data may therefore be within reach and could have a big impact on cybersecurity. "I would not be surprised if there would be an international agreement coming with regards to AI and related areas, such as cybersecurity," says Ms. Schaake. "I think the momentum is there, and if you look at the G7 it's all democratic countries. They talk about the role of technology, so there's more momentum now than there probably was last year," a fact she attributes to a rapidly evolving field of diplomatic relations. "I think there's an understanding that it doesn't make sense to deal with the harms coming from global companies on a country-by-country level. Now the next step is actually shaping up new agreements, new kinds of shared definitions in order to actually do something about it," she adds.

PERSPECTIVE: THE EUROPEAN UNION'S AI ACT

pillsbury

The European Union unveiled its proposed Artificial Intelligence (AI) Act (the AIA) in April 2021, setting out a framework of AI classifications and potential AI regulatory requirements. Just as with data laws, businesses need to be careful rushing into AI. Be aware there is a fresh effort, like GDPR and data, for laws to catch up and regulate use of AI.

The AIA seeks to regulate "*AI Systems*" based on their risk profile. The Commission states that "*the vast majority*" of systems currently used will be considered "minimal risk" and will not be formally regulated. However, the new AIA encourages compliance with codes of conduct which are to be drawn up by the Commission and Member States.

For "limited risk" systems the AIA introduces transparency obligations, for example, to chat bots and deepfakes. For those deemed "high risk," specific regulatory obligations will be imposed, such as independent assessment and the application of the "CE" mark, or amendments to pre-existing regulatory regimes (e.g., those in place for product safety and medical devices).

At the time of its implementation, the GDPR's fines (€20 Million or 4% of annual revenue, whichever is higher) were described as "eye-watering". It remains to be seen what label will be given to the new AIA's even higher penalty of up to €30 Million or 6% of annual revenue.

The proposed AIA will also likely have global impact, as with GDPR, and could give rise to tensions between trading blocs such as those over data transfers between the US and Europe.

Rafi Azim-Khan
Partner, Cybersecurity, Data Protection & Privacy practice co-leader, Pillsbury

CHAPTER 3

EXECUTING AI: ETHICS, PRIVACY & THE HUMAN FACTOR

"I happen to be a big believer that the future of AI is really the true collaboration between a human and a machine."

AJ Abdallat
CEO, Beyond Limits

Corporations face a multitude of challenges in navigating the AI cybersecurity landscape, from technical complexities to human elements. In particular, there is currently a focus on the balance between machines and humans and ethical considerations, as well as compliance with varying data privacy regulations.

AI has led to a fear over job redundancies generally, and the same logic may well apply to its role in cybersecurity as detection of anomalies can be automated. But humans still play a large role in the equation as they implement and supplement systems. "I happen to be a big believer that the future of AI is really the true collaboration between a human and a machine," says Mr. Abdallat. "Ultimately, I believe that AI is going to create more jobs, because AI can open the doors for us to go after more creative problems and allow us to go after challenges that were not achievable by human individuals alone."

Awareness and training programs therefore translate into organizational capacity and capability to establish successful AI cybersecurity initiatives. Such areas also include having a proper data governance structure and data policies to ensure ethical behavior. There are numerous examples of companies scraping data in bulk off internet platforms and services, only to sell the information to law enforcement and others. "You have to ask yourself from a data privacy and ethical cybersecurity point of view, about the quality and (mis)treatment of individuals in commercial databases. Companies make far-reaching yet invisible decisions with great impact on people's lives," Ms. Schaake notes.

"We've seen increasingly that cybersecurity vulnerabilities are found lower down in the chain or maybe even in suppliers," says Mr. Koene. "It would be difficult to argue that you need to get access to everybody's personal data and still consider this to be a GDPR-compliant way of doing things." The establishment of corporate policies is therefore paramount to doing business ethically while improving cybersecurity. "I hope that, five years from now, there are established governance and legal frameworks that enable much greater trust that these AI technologies that are being implemented into the world around us are actually safe and reliable, and contributing to a just and sustainable world," says Ms. Newman. "I hope that's the direction we move in but I am fearful that we are implementing these before we have proper control over the systems and understanding of the ways in which they fail and just increasing the risk across sectors with disproportionate harm to people who are already disadvantaged."

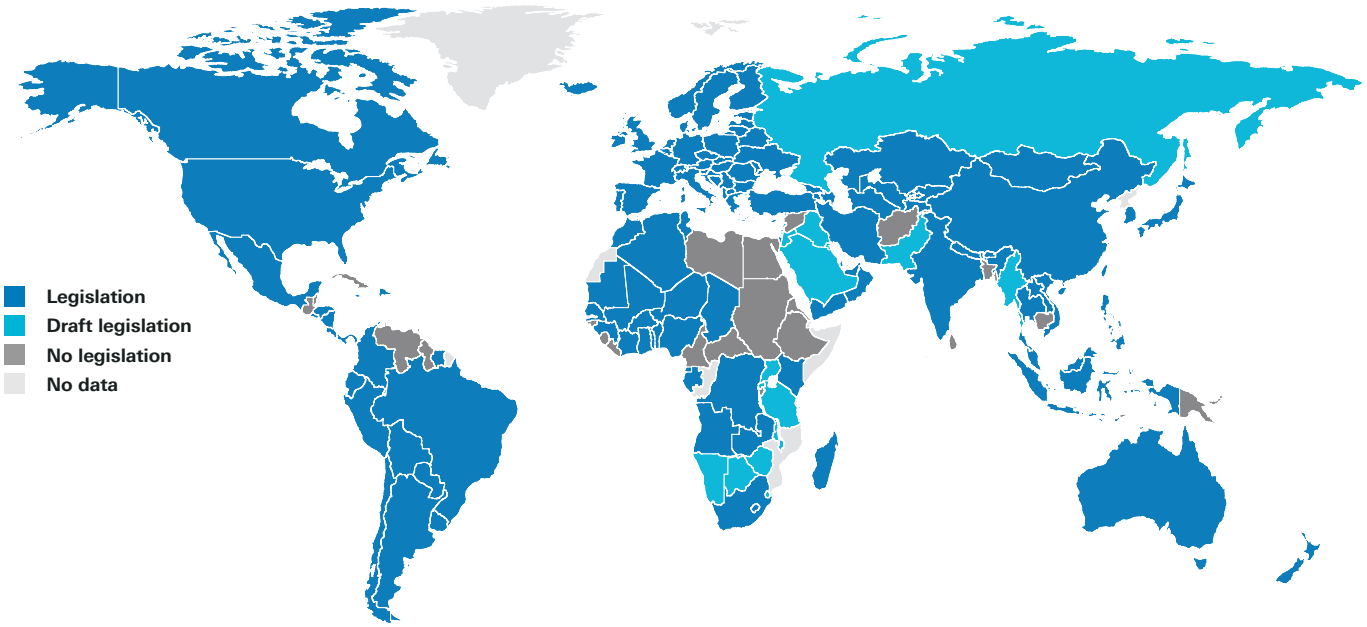
The global data privacy challenge

In the European Union and the European Economic Area, data privacy is a fundamental right and many other jurisdictions have followed suit. California adopted its Consumer Privacy Act in 2018, making it one of the stricter jurisdictions in the United States.[16] But it's the patchwork of different regulations across the United States—and also internationally—that creates a challenge for companies doing business across borders (see Figure 2). "A key element right now related to cybersecurity is the privacy of data and that is really going to be the major concern of all companies," says Mr. Abdallat.

Data regulations, as they relate to data privacy, therefore play an important role as organizations may have to limit the amount of data they can collect, use and store for cybersecurity purposes, particularly in places with strict regulations such as California and Europe. "Absolutely it is a disadvantage," Mr. Abdallat says about the difficulties of compliance with a patchwork of regulations across the United States (see Figure 3). "If we had a national system, it would allow us to focus on one uniform system because now, the resources I'm putting to basically look at 50 different sets of protocols and procedures, those resources can actually work on innovation and on deployment of solutions instead."

Figure 2

The state of data protection regulation around the world



Source: UNCTAD (2020)

The role and risks of AI in critical infrastructure

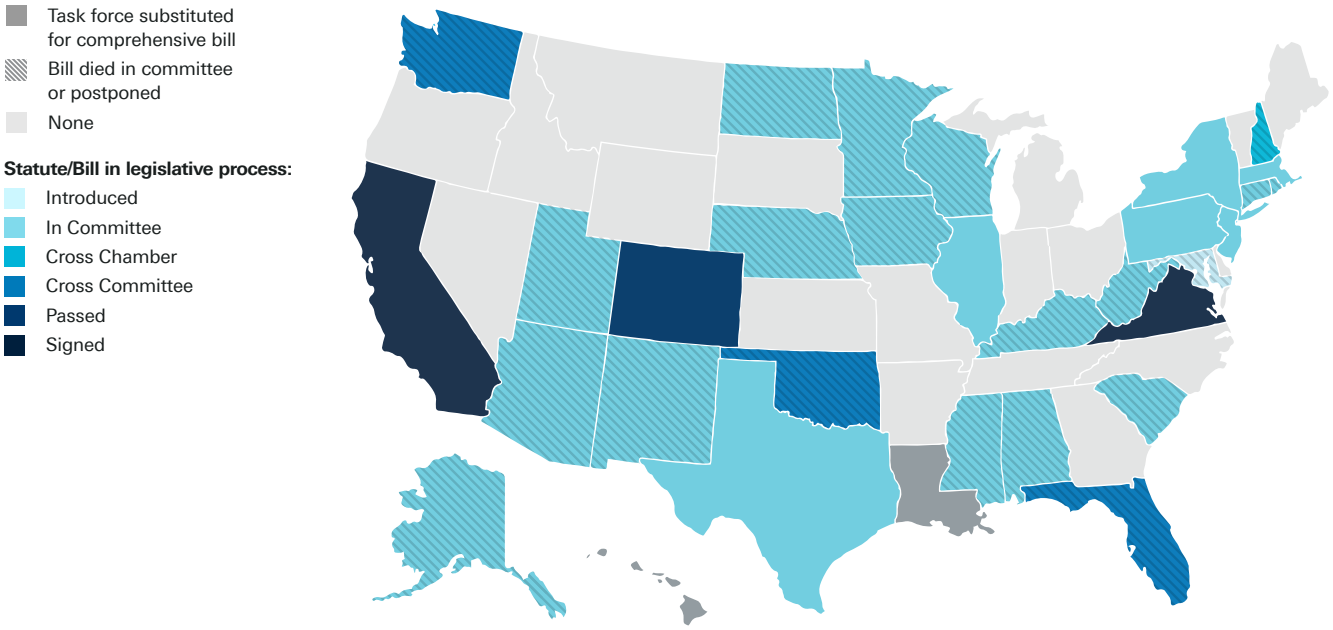
Certain sectors have more to gain—but also more to lose—from the role of AI in cybersecurity given their strategic importance and the amount of data they generate—both of which cause them to be larger targets for cyber incursions. "The current situation is pretty terrifying," says Jessica Newman, program lead at UC Berkeley's AI Security Initiative. "It is tempting to add machine learning tools into many business processes, and it is indeed becoming ubiquitous, but AI tools suffer from bias, vulnerability to attack, and a lack of explainability. Without proper governance and oversight, we are simply exposing industry, people, and the environment to significantly more risk." The recent ransomware attack on the Colonial Pipeline by hackers—which induced a gas supply crunch in the Southeastern US—is a prime example of cyberattacks on critical infrastructure that spill over into the physical world.[14]

In the United States, for example, there are 16 defined sectors considered critical infrastructure, such as financial services, energy and information technology.[15] Hence such sectors need to pay greater attention than the average organization to the possibilities of using threat intelligence and AI to improve their response to cyberattacks.

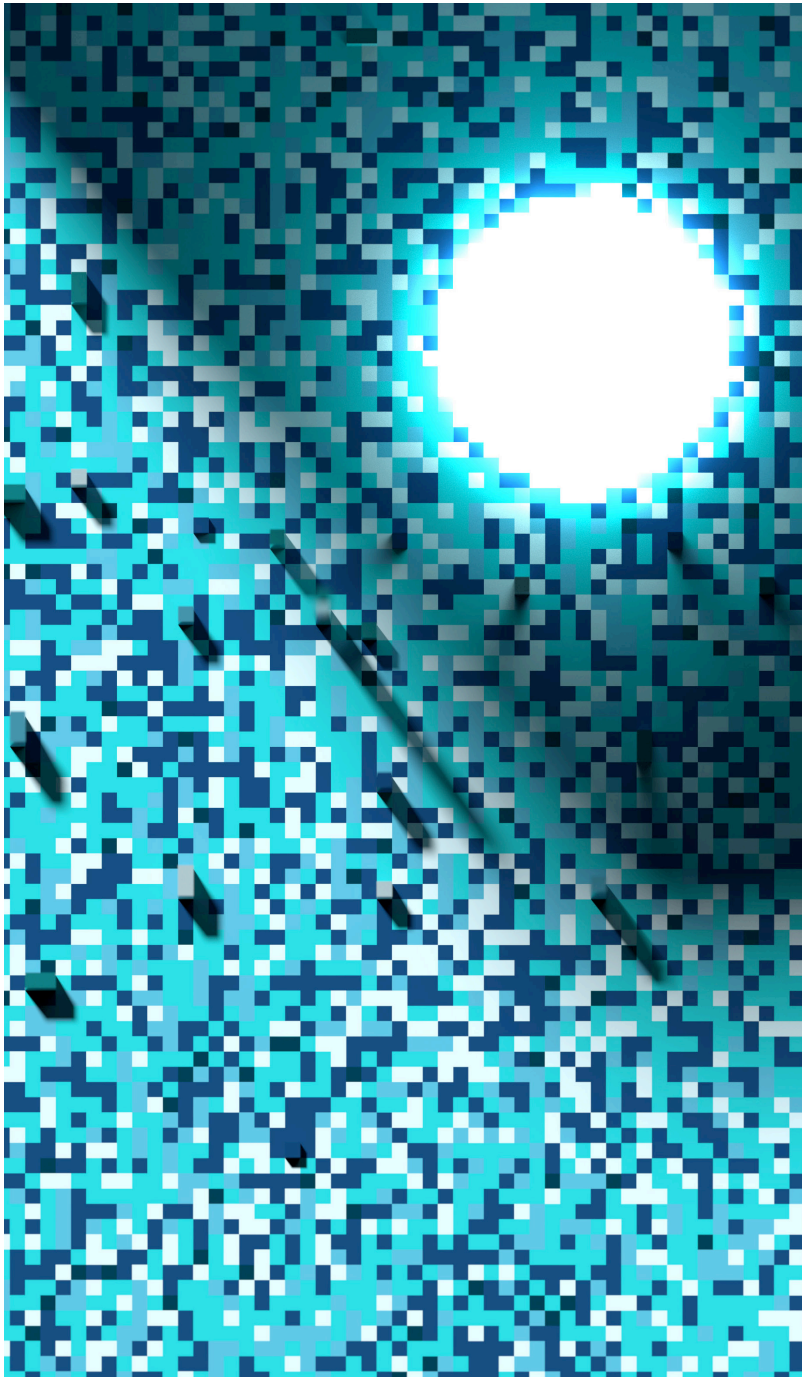
However, implementation is widely uneven, in part due to a lack of standards. "I would say readiness varies from industry to industry," says AJ Abdallat, CEO of Beyond Limits, an AI solutions company. "While there are many AI governance proposals and initiatives under development around the world, we do not yet have AI standards or overarching regulation to require and ensure that we have transparency to users, or broader society, or any kind of accountability when things go wrong," adds Ms. Newman.

Figure 3

Data privacy laws are making a slow march across the country



Source: IAPP (2021)



Beyond security: IoT, visibility and bias

The common connotation of AI related to cybersecurity relates to technology infrastructure; however, it is also recognized that such systems underpin a wide variety of applications to enhance cyber defenses more generally. Physical security, for example, is important as potential intruders can use in-person ways to gain access to corporate networks. This is particularly important to some sectors—such as energy, transport and real estate—in light of the rise of smart cities that rely on technologies such as facial recognition and various sensors.

"Oil and gas, utilities, and renewables are undergoing a so-called energy revolution in which the energy system is becoming cleaner, more distributed and more efficient and at the core of that transition is digitalization," explains Leo Simonovich, vice president & global head of industrial cyber and digital security at Siemens Energy. A key component of the transition is the implementation of sensors used by the Internet of Things (IoT). According to Ericsson, a Swedish multi-national network and telecommunications company, such devices will increase from 12.4bn in 2020 to 26.4bn by 2026.[17] "Each of those devices presents a potential vulnerability with all this complexity but AI offers enormous promise because the core challenge that needs to be solved is around visibility," says Mr. Simonovich.

Visible or not?

Machine-learning systems that leverage biometric and other forms of sensitive data are also growing in importance as companies contend both with know-your-customer requirements and competitive pressures to target their consumers more effectively. This is opening up new avenues for fraud, privacy breaches and other instances of malfeasance. "AI systems may appear to be doing really well at image recognition but are using features within the image that are quite alien to the way in which we humans look at the image," says Mr. Koene. "In principle, that doesn't necessarily mean there's a problem as far as using the system is concerned, but it does mean that you can manipulate images in a way that doesn't appear relevant to us but that will certainly trigger the AI system to generate a different kind of outcome," creating new risks.

Facial recognition policies and related identifiable technologies, such as biometrics, can still be of great importance to organizations but also face challenges when it comes to potential bias in AI and ML algorithms that may run afoul of regulations, create ethical issues, or present new challenges.

The human element

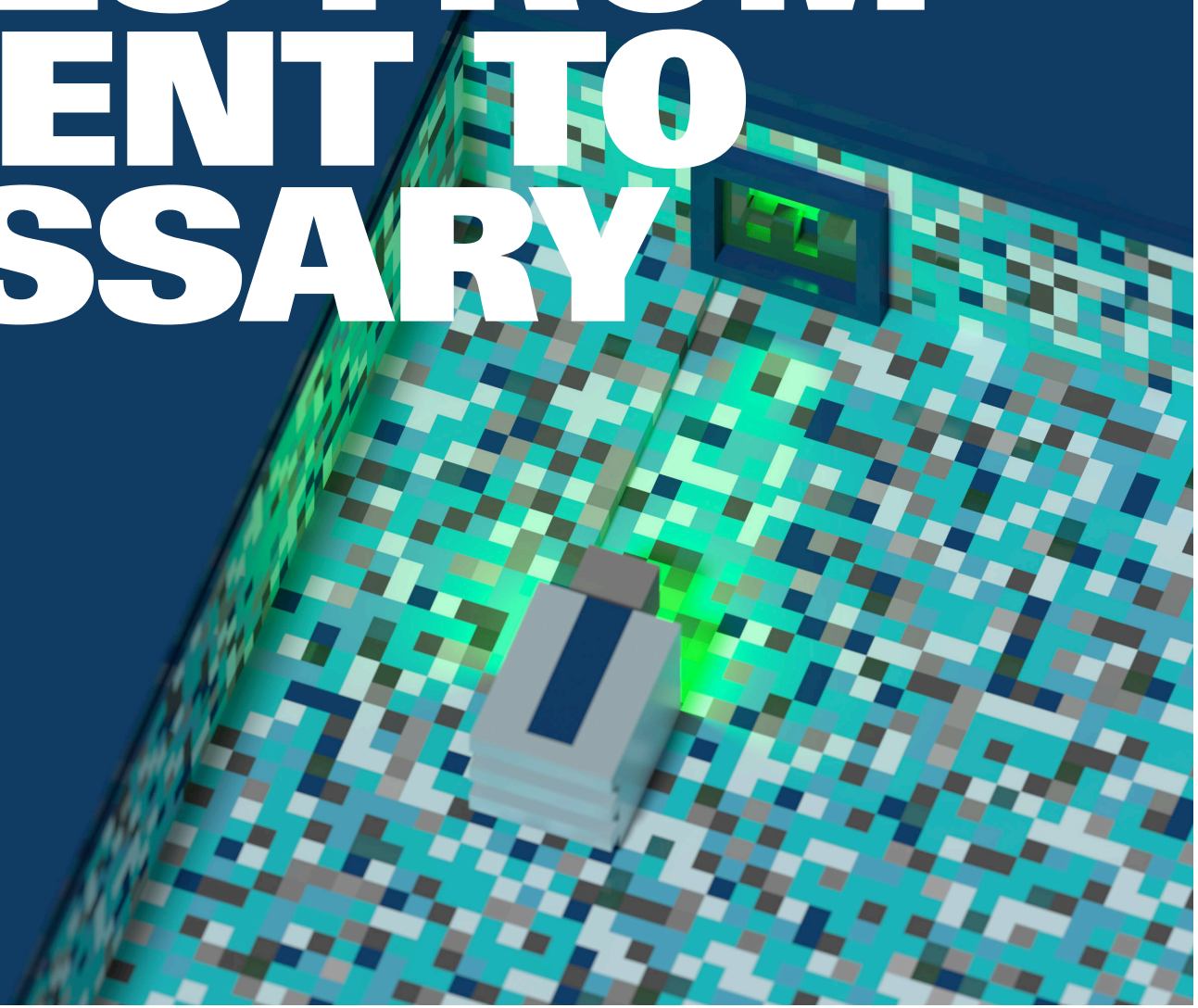
Leaving AI to fend for itself is not seen as a good practice due to the complexity of systems at various levels and a lack of current cognitive ability. "Taking decision-making out of human control while adding technical complexity might create a lack of complete transparency into how systems work, making it harder to fully understand, control and monitor them," says Ms. Newman. "We easily forget the role of humans at every stage right now of the AI life cycle in making the decisions of how to train these models and what to optimize them for, and how to put them into use and for what types of purposes."

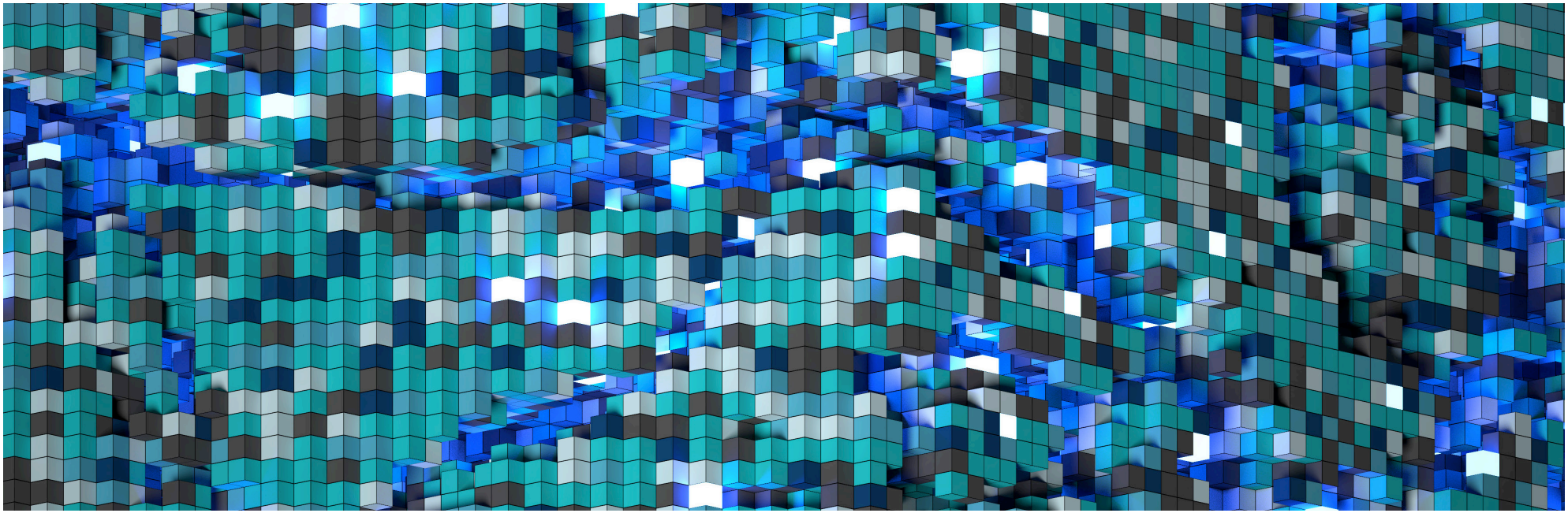
It is therefore imperative to remember the human aspect and decisions that go into the successful implementation and use of AI with regards to cybersecurity. "The problem with AI is that you're going to lose the ability for what I call human hunches or gut feelings," says Mr. Abdallat, "because now you're relying more on algorithms and machines." As a result, his company takes a data-driven AI approach that is supplemented by human knowledge. "We champion a hybrid approach of AI to gain trust of users and executives as it is very important to be able to have explainable answers," he says, meaning the need to know how conclusions were reached. A pure data-driven approach will provide answers, but cannot explain how those conclusions were reached or produce an audit trail, both of which provides confidence in the ultimate solution. "You need a partnership approach and then clear and compelling use cases that encourage adoption where you combine human capital and expertise with the technology to drive business outcomes," agrees Leo Simonovich, vice president & global head of industrial cyber and digital security at Siemens Energy. "You get the upper hand by making sure that you really get a good handle on data policies and knowledge management policies and procedures," says Mr. Abdallat. "Keeping humans in the loop is important, but you want to minimize that at the same time." The balance and interdependency of AI and humans therefore emerges as a key factor towards successful cybersecurity in which trust, transparency and accountability supplements the benefits of machines. "We don't let the machine learning algorithms run without humans," says Ms. Shivanandan. "We still need that human presence to evaluate and adjust our model based on actual things that are happening."

> "Taking decision-making out of human control while adding technical complexity might create a lack of complete transparency into how systems work, making it harder to fully understand, control and monitor them."
>
> **Jessica Newman**
> Program lead, AI Security Initiative, UC Berkeley

CHAPTER 4

AI GOES FROM NASCENT TO NECESSARY





There is widespread agreement that there is an important role for AI when it relates to cybersecurity, and the adoption is likely to increase over the next five to seven years as organizations realize its benefits. "Cybersecurity has grown a lot because of AI, and we're going to see tremendous growth in this area as we implement new techniques," says Mr. Abdallat. For example, an emerging number of solution providers use machine learning tools to offer continuous monitoring and evaluation of third-party vendors and suppliers to make companies more secure by informing them how secure their partners are. "We're only as good as the weakest link," says Mr. Simonovich. "We need partnerships to address sector-level challenges to create collective defense and AI has to be at the core of it in order to protect small- and medium-sized enterprises because they could potentially be exploited as a source of vulnerability."

At the same time, as the complexities of systems increase, cyberattackers will be quick to exploit them and potentially use AI themselves to penetrate systems. "The first challenge is that we are adding this complexity without proper control or oversight, and we're complicating the goal of cybersecurity to protect these broader systems that we rely upon," adds Ms. Newman.

The landscape is changing rapidly. "In the next five years, I think we will learn a lot more about new vulnerabilities that come from, for example, the wider rollout of the Internet of Things for many more connected devices that are plugged in easily, connected easily, but much less protected. And we will find how one weak link can sort of poison an entire system," says Ms. Schaake.

AI is therefore seen as augmenting, rather than replacing, humans. "The technology is not at the point where people should trust that removing a human from that loop would result in an optimum outcome," says Ms. Newman. A hybrid approach that's taking advantage of an AI data-driven model, but also human knowledge and engineering combined with an appropriate set of policies emerges as a win-win situation as it relates to enhancing cybersecurity. "AI can help overcome this idea of alert fatigue, do analysis at scale, get answers more quickly, bring context and insight, because ultimately what humans need to focus on is precision defense," says Mr. Simonovich.

"I think companies that invest in creating a strong infrastructure with policies and invest in training management and people are going to succeed whereas others who are taking it lightly are coming to the short end of the stick," says Mr. Abdallat. "You want to find that right balance, where you want to minimize the number of people that need to get involved, so you're reducing your risk, but at the same time, you have oversight—and you also still have human involvement."

REFERENCES

1 "INTERPOL report shows alarming rate of cyberattacks during COVID-19", INTERPOL, August 4th 2020.
2 "Cost of a Data Breach Report 2020", IBM, 2020.
3 "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor", FireEye Threat Research, December 13th 2020.
4 "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack", NPR, April 16th 2021.
5 "State-sponsored cyberattacks: Cybersecurity Tech Accord and Economist Intelligence Unit study reveals they are a major concern for businesses", Tech Accord, February 22nd 2021.
6 "Artificial Intelligence and cybersecurity", CEPS, April 21st 2021.
7 "From Roadblock to Scale: The Global Sprint Towards AI", IBM, 2020.
8 Wayne Thompson, Hui Li and Alison Bolen, "Artificial intelligence, machine learning, deep learning and more", SAS, n.d.
9 Steve Durbin, "How Criminals Use Artificial Intelligence To Fuel Cyber Attacks", Forbes, October 13th 2020.
10 "Artificial Intelligence Cybersecurity Challenges", ENISA, December 2020.
11 "Artificial Intelligence Index Report 2021", Stanford University Human-Centered Artificial Intelligence, March 2020.
12 Sarah Box, "How G20 countries are working to support trustworthy AI", OECD Innovation Blog, July 24th 2020.
13 Eve Gaumond, "Artificial Intelligence Act: What Is the European Approach for AI?", Lawfare, June 4th 2021.
14 Lauren Egan, "White House urges Americans not to hoard gas as hacked pipeline remains shut", NBC news, May 11th 2021.
15 Critical Infrastructure Sectors
16 California Consumer Privacy Act (CCPA)
17 "IoT connections outlook", Ericsson, n.d.

ABOUT PILLSBURY

Pillsbury Winthrop Shaw Pittman LLP is an international law firm with a particular focus on the technology & life sciences, energy, financial, and real estate & construction sectors. Recognized as one of the most innovative law firms by *Financial Times* and one of the top firms for client service by BTI Consulting, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their authoritative commercial awareness.

Pillsbury helps clients around the world seize the unique opportunities presented by artificial intelligence and fundamentally change and improve the way they operate. Our multidisciplinary AI team advises companies—from startups to global corporations, across all industries—and government agencies on navigating the technical complexities of this game-changing innovation as well as the evolving regulatory and legal standards that apply to it. Whether in relation to machine learning, natural language processing or neural network projects, we work hand-in-hand with AI inventors, early adopters and investors to address the full range of commercial, regulatory and liability concerns they encounter.

The firm has also earned a standout reputation for the keen insight and steady guidance it offers in connection with cybersecurity, data protection and privacy law issues. Pillsbury lawyers advise public and privately held businesses on all manner of critical data privacy issues, with particular experience in the technology, energy, financial, communications, defense/government contracts and health care sectors, as well as with critical infrastructure generally. Our multinational team of regulatory authorities, litigators, transactional lawyers, intellectual property counsel, government contracts practitioners and legislative strategists work closely with clients worldwide to monitor the rapidly changing data and cyber landscapes and tackle related security challenges.

For more information,
visit www.pillsburylaw.com