TAG Cyber

Security Annual

2023

SPECIAL REPRINT EDITION

REVOLUTIONARY MICROSHARDING TECHNOLOGY AND CYBERSECURITY

AN INTERVIEW WITH JOE SORIAL
VP PRODUCT, SHARDSECURE

CYBERSECURITY IN THE SPACE DOMAIN: SAFEGUARDING OUR FUTURE

WHY AI-BASED CYBERSECURITY WILL CONTINUE TO NEED THE HUMAN TOUCH

TAG CYBER DISTINGUISHED VENDOR

SHARDSECURE

The need to reduce cyber risk has never been greater, and ShardSecure has demonstrated excellence in this regard. The TAG Cyber analysts have selected ShardSecure as a 2023 Distinguished Vendor, and such an award is based on merit. Enterprise teams using ShardSecure's platform will experience world-class risk reduction—and nothing is more important in enterprise security today.

The Editors,
TAG Cyber Security Annual
www.tag-cyber.com

REPRINTED FROM THE TAG CYBER SECURITY ANNUAL

AN INTERVIEW WITH JOE SORIAL
VP PRODUCT, SHARDSECURE

REVOLUTIONARY MICROSHARDING TECHNOLOGY AND CYBERSECURITY

More organizations are moving to cloud-based storage in this digital transformation era, presenting a new frontier of data protection issues. Addressing these challenges, ShardSecure® has developed a pioneering Data Control Platform that promises enhanced security, privacy, resilience, and regulatory compliance for data in the cloud. During a recent conversation with ShardSecure, they shed light on the intricacies of their platform, discussing its key strengths in addressing the unique security challenges the cloud presents. They further illuminated how their innovative Microsharding technology not only obfuscates data but also makes it unattractive and unrewarding for potential breaches. By dispersing data across multiple clouds and rendering individual shards useless in isolation, ShardSecure has forged a game-changing path in data security, paving the way for a safer, more secure digital future.

With a simple, agentless implementation, the ShardSecure platform simplifies data security and privacy without legacy solutions' deployment headaches and performance drawbacks. Our "set and forget" management and policy-driven approach also helps companies maintain flexibility as data storage grows and new data privacy regulations arise.

TAG Cyber: Can you provide an overview of ShardSecure's Data Control Platform?

SHARDSECURE: At ShardSecure, we believe that all organizations can secure and protect their data wherever they want—whether on-prem, in the cloud, and in hybrid- or multi-cloud architectures. In the face of increasing cyberattacks and operational complexity, we help companies simplify data security and protection.

With strong data privacy, robust data resilience, cross-border regulatory compliance, native ransomware protection, and simple, agentless integration, the ShardSecure platform offers a multifaceted solution to complex challenges.

TAG Cyber: What specific data security challenges does ShardSecure's platform address?

SHARDSECURE: Until now, organizations had few options to secure their unstructured data and prevent third-party access in the cloud. Current solutions are resource-intensive, and new technologies like machine learning and AI require organizations to store more business-critical
data in the cloud. With the challenges of complex data privacy laws and a rapidly evolving regulatory landscape, securing and protecting data in the cloud presents a major obstacle for most organizations.

Legacy solutions typically address a single aspect of data protection, privacy, or resilience, but data security needs to extend to every part of the organization. These solutions also tend to introduce significant complexity, performance drawbacks, and the need to update existing data flows and applications. Companies need new solutions fast—for privacy, compliance efforts, and security teams trying to keep data safe from exfiltration and attacks. The ShardSecure platform gives organizations the freedom and flexibility to store their data anywhere while rendering it unintelligible to unauthorized users.

With a simple, agentless implementation, the ShardSecure platform simplifies data security and privacy without legacy solutions' deployment headaches and performance drawbacks. Our "set and forget" management and policy-driven approach also helps companies maintain flexibility as data storage grows and new data privacy regulations arise.

TAG Cyber: How do you ensure secure data handling/storage without compromising usability or performance?

SHARDSECURE: Traditional data sharding inspired ShardSecure's patented Microshard™ technology. Alongside tools like

ElasticSearch and MySQL, sharding, i.e., fragmenting data into small pieces and then distributing those pieces to multiple storage locations for faster performance, is favored by storage and database companies like Oracle, Altibase, and MongoDB. ShardSecure's Microsharding techniques build upon the benefits of traditional sharding by introducing numerous data security, resilience, and compliance capabilities. We achieve high throughput and low latency by reading/writing in parallel and compressing pointers. Data security almost always brings a performance cost, but ShardSecure is a notable exception.

The ShardSecure platform also ensures data security without compromising usability. Acting as an abstraction layer, our technology operates with minimal impact on operations teams. Plus, there's no need for agents or disruption to application and data flows. ShardSecure's native multi-cloud and hybrid-cloud support also provides a single interface to manage storage locations and move data—without impacting performance.

TAG Cyber: How does the company's technology enable organizations to strengthen data security and resilience?

SHARDSECURE: ShardSecure strengthens data security by rendering data unintelligible to unauthorized users. Our innovative approach to file-level encryption works by shredding and distributing data to multiple customer-owned storage locations. By using an API-based abstraction layer between an organization's applications and its storage infrastructure, we ensure the security of that data.

ShardSecure's platform also supports robust data resilience, including multi-cloud architectures. Our technology maintains data integrity and availability during disruptions like cloud provider outages, misconfigurations, and ransomware attacks. Other solutions typically mirror data to achieve redundancy and resilience, which increases storage costs. Our algorithms, however, are based on a cost-effective architecture.

First, we maintain high availability. Each instance of ShardSecure is a virtual cluster that can be run on-prem or in the cloud, and customers can configure two or more virtual clusters for failover. Second, we maintain data integrity by performing multiple checks to detect unauthorized modifications and by self-healing data to transparently reconstruct it after malicious or unauthorized tampering or deletion. The result is accurate, available, and confidential data, regardless of storage location.

TAG Cyber: What is ShardSecure's approach to data privacy and compliance?

SHARDSECURE: The traditional approach to maintaining data privacy is fortifying data segmentation. ShardSecure's technology desensitizes the data, rendering PII and other sensitive material unintelligible to unauthorized users—from cloud storage admins to attackers. This approach mitigates the impact of data breaches, strengthens data privacy, and ensures compliance with cross-border regulations.

ShardSecure's platform enables organizations to address data sovereignty and residency concerns by utilizing their preferred cloud storage providers in their desired geographic locations and jurisdictions.

Organizations can distribute data across different regions of a single cloud provider, multiple cloud providers, or a hybrid mix of on-prem storage and one or more cloud providers.

ShardSecure is also validated to meet the requirements of Use Case 5 for Schrems II/European Data Protection Board (EDPB) compliance. Our split processing technology is easily deployed in a multi-party processing environment, allowing organizations to store and process data safely under Use Case 5.

With our innovative approach to data security, privacy, resilience, and compliance, ShardSecure offers a new way for companies to face modern cyber challenges and regain data control.

CYBERSECURITY IN THE SPACE DOMAIN: SAFEGUARDING OUR FUTURE

SPACE CENTER HOUSTON

International Space Center Mission Control

DAVID NEUMAN

In the quiet and bustling offices of the International Space Station's control center in Houston, Texas, a tension-filled silence suddenly hung in the air. The screens in front of the control team flickered, shifting from the usual display of telemetry data to an ominous black. Only a single line of text remained: "Access granted. Control transferred."

A thousand kilometers above, the International Space Station (ISS) began slowly veering off its usual orbital track, unbeknownst to the astronauts living and working inside. Meanwhile, thousands of kilometers below, another significant event was taking place.

Simultaneously, the global positioning system (GPS) ground stations, a constellation of 24 satellites traveling 12,000 miles above the Earth to provide positioning data to billions of users around the globe, started reporting unexpected anomalies. This wasn't an isolated error; all 24 satellites were rapidly rendered non-operational. The lifeblood of navigation and timestamping systems worldwide was effectively silenced.

Down on Earth, the impacts of this double-edged attack were almost immediate. Air traffic controllers stared at their screens in bewilderment as the positional data of thousands of planes disappeared.

Ships at sea lost their bearings, and self-driving vehicles on the streets came to a bewildered halt, unable to pinpoint their location. Stock markets experienced extreme turbulence as high-frequency trading systems faltered.

In the backrooms of power grids, engineers watched in horror as synchronization of the grid, which relied on GPS timestamps, started to fail, causing blackouts in cities worldwide. At the same time, billions of smartphone users were suddenly unable to access location-based services, severely disrupting daily life and business operations. The world had been rendered blind and lost in space and time.

Contemplating the chaos of a major cyberattack on space technology may be easier than trying to imagine a coordinated response.

At the ISS control center, the staff desperately tried to regain command of the space station. Their concern was not just for astronaut safety but also for the dozens of crucial scientific experiments onboard, many of which had implications for climate research and future space exploration. As the ISS continued its unintended and risky orbital maneuver, the specter of the uncontrollable descent of the 420,000 kg station towards Earth loomed, with potentially catastrophic consequences for those on board and those in the projected impact zone on Earth.

Suppose this hypothetical scenario had actually happened. What would come next?

Chaos would have erupted in the civilian world and within the corridors of power, both domestic and international. A flurry of activity would have begun within various government agencies in the United States. The Department of Homeland Security would have quickly mobilized to protect and coordinate a response to cyberattacks against terrestrial components of the space systems.

And so it went. As they worked tirelessly to manage the impact on civilian infrastructure, the Federal Bureau of Investigation launched a parallel investigation, seeking to identify the perpetrators of the cybercrime. Simultaneously, the Department of Defense, in coordination with the U.S. Space Force and U.S. Cyber Command, focused on the defense of national space systems. Their immediate goal was to restore control of the International Space Station and the GPS satellites while securing other space-based assets against potential follow-up attacks.

The National Reconnaissance Office, tasked with operating intelligence satellites, was also in high gear, scanning through petabytes of data to ascertain if the attack originated from a foreign power. Meanwhile, the National Aeronautics and Space Administration (NASA) provided technical support, applying its extensive expertise on the ISS to help regain control of the wayward space station.

Despite this flurry of activity, there was a palpable sense of confusion and tension due to overlapping jurisdictions and the need for defined responsibilities. It needed to be made clear who should be taking the lead, causing delays in the response and creating friction between agencies. With its responsibility for commercial spaceflight, the Federal Aviation Administration felt sidelined despite the significant impact on commercial aviation and navigation systems.

Internationally, the response was even more fragmented. Nations dependent on GPS scrambled to mitigate the impacts. Discussions started at the United Nations about the need for an international framework for space cybersecurity. The spacefaring nations, each with its own stake in space assets, urgently convened to discuss a joint response. But the absence of an international body with clear responsibility and authority to respond to space-based cyberattacks added another layer of complexity and delay.

This hypothetical is indeed the stuff of science fiction. And yet, it represents a plausible threat in our increasingly interconnected and space-reliant world. The repercussions such an event could have on society and businesses worldwide, from disrupting air travel and telecommunications to causing catastrophic power failures and affecting financial markets, are alarming.

Our future on Earth and in space is irrevocably tied to our ability to safeguard these crucial systems from cyber threats. Hence, the need for technological solutions and international cooperation, for norms and defined responsibilities in this rapidly growing field. This is not merely about preserving the status quo; it's about securing a future where space continues to be a resource that unites nations, propels economic growth, and catalyzes scientific discovery.

WE ARE INTERTWINED WITH THE SPACE DOMAIN

Our entanglement with these space systems stretches far wider and deeper into our everyday lives and societies than one might initially realize. A look at satellite communications, weather forecasting, climate monitoring, and other dependencies throws this into stark relief.

An attack on satellite communications, the backbone of global connectivity, would go beyond merely obstructing GPS navigation. It would cripple services like TV broadcasts, internet connectivity, and long-distance telephony. This would be particularly detrimental to remote and rural areas, where traditional infrastructure may not reach, potentially isolating entire communities.

Simultaneously, our ability to predict and prepare for severe weather conditions could be dramatically hampered if the satellites that monitor weather patterns and climate trends were compromised. Such an event would not only impair our ability to provide life-saving early warnings for hurricanes or monsoons, it could also compromise our long-term understanding of climate change, with far-reaching implications for the planet.

Similarly, an attack on space-based systems that support precision agriculture, global financial systems, emergency services, and scientific research would prove devastating. Farmers could face massive agricultural losses without the weather data they rely on. Disruptions in the precise timestamping provided by GPS satellites could send shockwaves through global stock exchanges and banking transactions, potentially triggering widespread economic instability. Additionally, we rely on emergency services for safety and security, such as fire, police, and ambulance services, which could significantly increase response times without reliable navigation systems. Finally, pursuing knowledge could be stalled, as researchers across various fields—from wildlife migration to astronomy—rely heavily on satellite technology for data gathering and observation.

THE COMPOSITION OF SPACE SYSTEMS AND OPERATIONS

This extensive network of dependencies highlights the need for robust and proactive measures to safeguard space-based assets from the looming threat of cyberattacks. Protecting space systems requires cyber defenders to fully grasp intricate operations and interconnections. Like an enterprise, these systems contain many connected components, each potentially a vulnerability that adversaries could exploit. Comprehending how they fit together, function, and interact is key. It empowers defenders to anticipate threats, implement protections, and maintain resilience.

Securing assets from cyber threats isn't just about guarding individual components. It's about protecting an entire ecosystem, which demands a holistic understanding of the system's architecture and operations. In the intricate ballet of global communication, space-based assets such as satellites, space telescopes, and space stations perform their dance high above the Earth. Each celestial body houses its onboard systems.

Think of these as the asset's brain—containing computer processors, storage, sensors, and communication antennas. Some even have thrusters for maneuvering. This array of onboard systems receives commands from Earth and manages the assets' daily operations, ensuring the harmony of their orbital dance.

On the Earth's surface, the dance partners of these space assets are the ground stations, each equipped with large antennas. Positioned strategically around the world, they maintain a constant pas de deux with the satellites, undeterred by the Earth's rotation. Here is where the conversation happens—ground stations dispatch commands to the satellites and, in return, receive a cascade of data. They function as the essential terrestrial connection points in this vast space communication network, transmitting and receiving signals like the ebb and flow of an electromagnetic tide.

But the dance does not end there. The data, once received, embarks on a new journey, coursing through terrestrial networks toward data centers scattered across various locations. The frequencies and technologies forming these communication links vary, fine-tuned for the type of satellite and its distance from Earth. The information is processed, stored, and analyzed in these data centers, converting the raw data into a comprehensible format for further use.

Finally, these data centers also take on the pivotal role of a command hub, from which operators send instructions to the space-based assets. This intricate network, stretching from the silent void of space to the bustling data centers on Earth, forms a complicated choreography far more elaborate and interconnected than traditional technology systems. Understanding this network is vital to appreciating the sophistication of our modern space infrastructure, and the vulnerabilities that must be secured to protect it.

THREATS TO SPACE OPERATIONS

While specific details about cyberattacks on space systems are often classified or undisclosed due to national security concerns, several recent incidents shed light on the types and severity of such threats. These real-world attacks illustrate the diversity of the space ecosystem's cyber threats, ranging from service disruption to espionage. The threats can come from various sources, including nation-states, non-nation threat actors, and individual hackers. (I have created below a timeline of recent space-related attacks, including published attributions of the attackers.)

Why is space particularly susceptible to cyber threats? While space assets share similarities with those affecting terrestrial systems, several factors make them uniquely vulnerable. Assets such as satellites are designed to operate for many years, sometimes even decades. This longevity means their onboard security can quickly become outdated, making them more vulnerable to evolving threats. Once a satellite is in orbit, it's virtually impossible to physically access it for repairs or upgrades. Therefore, any security vulnerabilities present at launch, or those that arise due to changing threat landscapes, can't be rectified.

Due to the inherent latency in communication with space assets, and the limited processing capabilities of many satellites, sophisticated real-time intrusion detection and response measures take time to implement. The radio signals used for satellite communication can be relatively easy to intercept, jam, or spoof, especially those of lower-frequency bands, unless protected by strong encryption and authentication measures. Components for space assets often come from a global supply chain, increasing the risk of compromised hardware or software being included in the final product.

Given these challenges, cybersecurity in the space domain requires specialized strategies and solutions that go beyond the measures employed in traditional IT systems. It calls for secure design and manufacturing advances, robust encryption and authentication protocols, secure and reliable command-and-control systems, and international cooperation to establish space-specific cybersecurity norms and practices.

SECURING SPACE AGAINST CYBERATTACKS

As we extend our reach into the cosmos, security becomes paramount. This reality is rendered more pressing as the scope of our space economy continues to expand. The 5,400 satellites currently in orbit will be dwarfed by the anticipated launch of more than 24,500 satellites over the next decade. Commercial ventures will account for over 70% of these new celestial bodies.

The escalating significance of these assets to the global infrastructure, and the mounting sophistication of cyber threats, underline the urgency for innovative solutions. However, the unique hurdles presented necessitate a different approach than we typically employ to tackle traditional cybersecurity issues.

Several solutions are emerging, each addressing the specific cybersecurity demands of the space domain. Quantum encryption, for instance, is leading the way in communication protection between space assets and ground stations, as traditional encryption methods risk obsolescence in the face of advancing quantum computing. AI and machine learning are emerging as invaluable tools for real-time threat identification, sifting through massive data sets to improve response times and system resilience.

As our space assets multiply, secure space traffic management is becoming increasingly vital for identifying potential cyberattacks and ensuring safe operation. A commitment to cyber resilience in space systems design is essential. Building these systems with cybersecurity as a cornerstone from inception will help ensure they can withstand future threats.

In an increasingly interconnected world, establishing international cybersecurity standards for space could unify and enhance the security of all spacefaring nations and companies. And leveraging blockchain technology could help secure the integrity of hardware and software used in space systems, mitigating a significant source of the threats.

Finally, strengthening the security of land-based components, such as ground stations and data centers, is crucial to a holistic space strategy. By integrating these innovative technologies and approaches, we can fortify the cybersecurity of the space domain, securing the critical services we rely on now and will continue to rely on in the future.

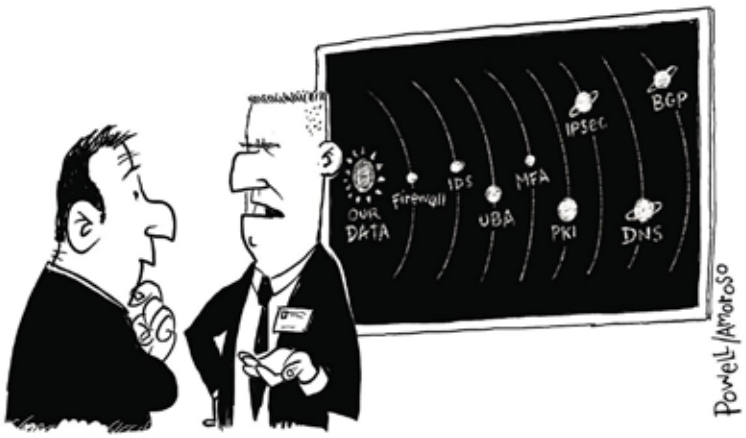
THE TAKEAWAY

My hypothetical cyberattack was designed to serve as a sobering reminder of the potential vulnerabilities and profound consequences of such an attack on our space-based systems. I hope it underscored thought-provoking questions about our preparedness, the interconnectedness of our world, and the urgent need for action.

Moreover, the response portrayed in our scenario highlights the challenges of coordinating a timely and effective counter to space-based cyber threats. Overlapping jurisdictions, a lack of defined responsibilities, and the absence of international protocols create confusion and delays, leaving us vulnerable. It emphasizes the critical need for collaboration and clear lines of authority to ensure a swift and coordinated response.

I hope the scenario also underscored the unique nature of space as a domain for cyber threats. The longevity of space assets, the difficulty of access for upgrades, and the global supply chains make them particularly susceptible to evolving risks. We must recognize the distinctive characteristics of space systems and develop tailored strategies to protect them from threats that transcend traditional cybersecurity approaches.

Our future, on Earth and beyond, is inseparable from the space domain. It is time for governments, organizations, and individuals to prioritize the protection of our space-based systems and preserve the benefits they bring. Will we unite to strengthen resilience, foster international collaboration, and establish robust frameworks to defend against space-based cyber threats? The answer will shape the future of our interconnected world and determine whether space remains a beacon of unity, innovation, and exploration.



"Uh, yes – I will admit some NASA influence in the new security architecture."

WHY AI-BASED CYBERSECURITY WILL CONTINUE TO NEED THE HUMAN TOUCH

DAVID HECHLER

It strikes me as almost a foregone conclusion that artificial intelligence will transform cybersecurity. But it's far less clear, at least to me, whether the result will be a standoff between enemy forces that rely almost entirely on AI defenses.

It seems inevitable that there will be an AI arms race. There already is. The United States and China are the competitors mentioned most prominently in the media. Russia, North Korea and Iran are the other nation-states active in launching cyberattacks. They'll try to match the advances of their targets. Other countries could emerge in coming decades.

It's easy to argue that AI will figure into the equation more and more prominently—on both offense and defense. But that doesn't mean that the machines will be in control. AI will not be calling all the shots. At least not in the foreseeable future. Much about the way the competition evolves will depend upon the humans who collaborate with the technology. Just as it does when AI is used by the military (as I will discuss below).

A lot of the talk right now is about the astonishing technological advances. When the conversation turns to people, they are often engineers who are building the software, and leaders of companies that are funding it—and pushing the competition. These individuals are certainly enjoying a well-deserved moment. But they aren't the only ones who are important players in this realm.

Lawyers, philosophers, journalists, researchers and all kinds of academics have expressed concern about the dangers

AI may pose not only to our country, but to humanity. Far from being seen as our protector against cyberattacks, some people view AI as a grave threat to our future.

A widely cited **survey** produced by AI Impacts in 2022 asked researchers who had published papers presented at two large machine-learning conferences this question: "What probability do you put on future AI advances causing human extinction or similarly permanent and severe disempowerment of the human species?" Based on 738 responses, the median respondent said the chance was 5%. But the number that many news accounts cited was double that number because 48% of respondents said the chance was 10%, and that's the statistic almost everyone used.

"AI systems can neither design themselves nor clean their own data, which leads us to conclude that increased reliance on AI will make human skills even more important..."

"Would you work on a technology you thought had a 10% chance of wiping out humanity?" New York Times columnist Ezra Klein **wrote** in March 2023. Klein explained his deep concerns while acknowledging that the train has already left the station. And the challenge of slowing, much less stopping, its progress seems daunting at best. As apprehensions about ChatGPT have mounted, a chorus of voices joined his.

It's possible that politicians may try to gain some measure of control through legislation. But even if they were convinced of the need, the likelihood of success seems highly problematic. The work is in the private sector, and the funding is from companies like Microsoft, Google and Facebook. So government doesn't control all the purse strings. And if the government tries to create legal roadblocks, critics will almost certainly accuse it of handing China a devastating, and potentially deadly, gift.

But let's return to cybersecurity, where the aim is to use AI to safeguard our safety. The machine learning will need to be directed by humans who study the threats and feed relevant information into the technology. In my research, the article I came across that shed the most light on this subject was **Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War**, by Avi Goldfarb and Jon R. Lindsay (this is where my earlier reference to the military comes in). Writing in the journal International Security, the authors did touch on cybersecurity and cyberwar, but that's not why I found it relevant. When we're talking about cybersecurity in the broadest sense—including battles between nation-states—then war is more than an analogy.

Goldfarb and Lindsay don't address the cybersecurity challenges we're addressing here, but they do talk about the ways corporations and even doctors use AI. The authors see great value in the technology. They expect it to transform the world in which we live. But they don't see it substituting for humans. They anticipate a collaborative relationship that builds on the strengths of each. "A well-specified AI utility function has two characteristics," they write. "First, goals are clearly defined in advance. If designers cannot formally specify payoffs and priorities for all situations, then each prediction will require a customized judgment. This is often the case in medical applications. When there are many possible situations, human judgment is often needed upon seeing the diagnosis. The judgment cannot be determined in advance because it would take too much time to specify all possible contingencies. Such dynamic or nuanced situations require, in effect, incomplete contracts that leave out complex, situation-specific details to be negotiated later."

The authors go on: "AI adoption may radically change the distribution of judgment by altering who in an organization makes decisions and about what, but in all cases, humans are ultimately responsible for setting objectives, making trade-offs, and evaluating outcomes.... AI systems can neither design themselves nor clean their own data, which leads us to conclude that increased reliance on AI will make human skills even more important..."

There's another important factor concerning cybersecurity based on AI. The debate over ChatGPT may not involve the government, but the government is very much involved in the world of cybersecurity. And it will inevitably be deeply involved in budgetary and strategic decisions that involve AI. When Goldfarb and Lindsay write that "seemingly trivial procedures can become politicized when budgets and authorities are implicated," it's easy to see how this applies to cybersecurity. "Even in the absence of parochialism," they continue, "the complexity of administrative systems introduces interpretive challenges for personnel."

In the case of cybersecurity, there's plenty of personnel. The Cybersecurity and Infrastructure Security Agency, the National Security Agency and the Department of Justice all play important roles. The heads of those organizations and other appointed cybersecurity leaders don't report to AI. And their judgments affect how AI is deployed. When it comes time for lobbyists and government agencies to press representatives in the House and Senate to approve appropriations for cybersecurity tentatively slated to be included in the annual National Defense Authorization Act, they aren't likely to be glad-handed by ChatGPT.

Finally, let's not forget that the political winds in the United States have been shifting from administration to administration. There are no guarantees that new leaders will continue to support AI or a robust cybersecurity budget. A new administration's strategy could certainly change course. And the same could be true in other parts of the world. As hard as it is to predict the advances of the technology, it can be just as challenging to gauge the path that politics will take.

SHARDSECURE

ShardSecure is a cybersecurity company that specializes in Microsharding technology. Their revolutionary solution disassembles data, distributes the shards across multiple clouds, and renders them useless in isolation. By making data breaches unattractive and unrewarding, ShardSecure provides organizations with unparalleled security. The company, founded in 2018, has its headquarters in New York, USA.

TAG CYBER
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG CYBER SECURITY ANNUAL