TAG Cyber Security Annual 2022

SPECIAL REPRINT EDITION

SAFEGUARD YOUR PEOPLE, DATA, AND BRAND THROUGH DIGITAL RISK PROTECTION SERVICES

AN INTERVIEW WITH KAILASH AMBWANI, CEO, CONSTELLA INTELLIGENCE

CYBERWAR...THE DAY AFTER

IS THE GOVERNMENT'S VERSION OF ALL IN THE FAMILY A REALITY SHOW?

TAG CYBER DISTINGUISHED VENDOR

Constella INTELLIGENCE

The need to reduce cyber risk has never been greater, and Constella Intelligence has demonstrated excellence in this regard. The TAG Cyber analysts have selected Constella as a 2022 Distinguished Vendor, and such award is based on merit. Enterprise teams using Constella's platform will experience world-class risk reduction. 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

TAG CYBER | Constella

AN INTERVIEW WITH KAILASH AMBWANI, CEO, CONSTELLA INTELLIGENCE

SAFEGUARD YOUR PEOPLE, DATA, AND BRAND THROUGH DIGITAL RISK PROTECTION SERVICES

The business world's growing dependence on digital services continues to increase the volume and range of external digital threats aimed directly at executives, employees, brands, operations, and infrastructure. To respond, organizations must employ proactive measures to monitor malicious activity, collect intelligence and provide proactive, actionable guidance.

Constella Intelligence meets this challenge via Dome, an advanced digital risk protection platform that not only defends people but protects data and ensures the integrity of corporate brands. We were eager to learn more about these services and how they can be employed across an enterprise.

Many attack techniques aimed at executives also impact brand reputation, including impersonation profiles, fake social media content and hijacked accounts.

TAG Cyber: Why do employees need digital risk protection?

CONSTELLA: That's an excellent question, because many organizations assume that only senior executives are targets for external threats. In fact, every employee with access to valuable internal assets needs digital risk protection. While the volume of digital transformation initiatives multiplied rapidly in the years prior to 2020, that process accelerated at a staggering rate during the COVID pandemic—compressing seven years of development into just a few months, according to a McKinsey study. As a result, digital transformation now means that most knowledge workers have access to critical systems and data, even as they typically lack corporate-grade security practices and protections.

Threat actors know these trends, and the opportunity they present. That's why compromised credentials and exposed personal information now represent the most common vector for data breaches, and they enable account takeover (ATO), ransomware and phishing attacks. To be clear, executives and VIPs remain primary targets, and the visibility and status of these individuals mean a different level of threat. Executives face online impersonation, hacktivism, reputation attacks and doxxing, all of which affect brand and market value and, in extreme cases, personal safety for them and their families. Recognizing that executives and employees face different types of threats, we designed our Dome platform to provide two tiers of protection: Employee Protection for common threats aimed at employees, and Executive Protection for enhanced defenses against a broader range of attacks. We also ensured that the Dome platform had the massive scalability and automated, continuous monitoring to protect everyone with access to sensitive data and systems, regardless of the size of the organization.

TAG Cyber: How do these external threats extend to corporate brands?

CONSTELLA: Many attack techniques aimed at executives also impact brand reputation, including impersonation profiles, fake social media content and hijacked accounts. The difference is they target corporate, rather than individual, accounts and profiles. In addition, brands also face the threat of stolen intellectual property, counterfeit products and viral campaigns that can cause extended damage to the brand. Clearly, organizations need the ability to recognize and respond to attacks against their brand from impersonation sites, defacement of online properties or phishing campaigns

targeting customers. However, they also need to be able to know if malicious online activity originates in online communities where threat actors congregate, and understand the nature of the conversations in those closed forums or messaging platforms.

These capabilities will become even more essential as digital geopolitical threats grow in frequency and severity. The good news is that the same automated, continuous monitoring and analytics within our Dome platform that protect executives and employees also can monitor brand-related malicious activities, because we monitor thousands of sources across the surface, deep, and dark web as well as social media. Organizations gain the ability to identify these external risks targeting their brands sooner and respond proactively to limit damage.

TAG Cyber: Tell us more about how to address geopolitical threats.

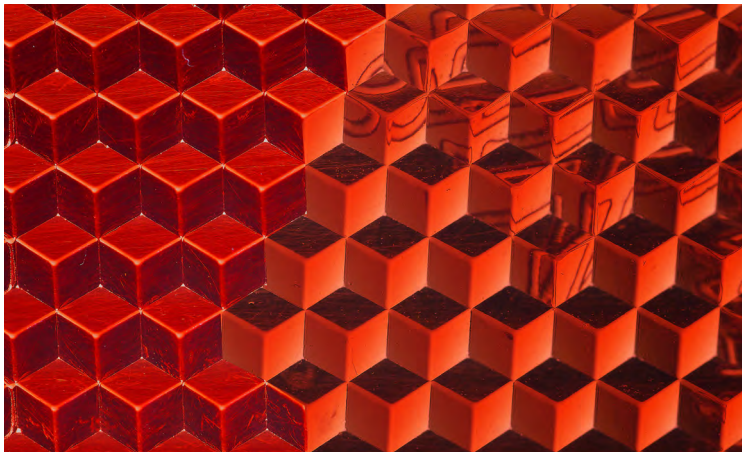
CONSTELLA: Geopolitical threats illustrate how multiple threat vectors intersect, such as a coordinated group of threat actors targeting an organization to discredit the executive team, steal data, damage the brand and launch a viral disinformation campaign. In short, all these techniques are now central components of international conflict.

Businesses need immediate insight into rapidly evolving political, economic and social situations within or across geographic regions to be able to minimize damage from geopolitical threats. Monitoring across a massive volume of data from diverse sources provides immediate awareness of everything from compromised credentials and exposed personal data on the dark web to fabricated social media content to discussions of floorplans of facilities. With this visibility, organizations can anticipate and defeat digital risks.

The scope of geopolitical threats has expanded rapidly over the last decade, with the volume of online threats surrounding the Ukraine invasion illustrating its scale and impact. That's why our Geopolitical Protection module in Dome provides automatic, scalable and continuous monitoring for regional and global geopolitical threats, including hostile narratives aimed at brands or individuals. This intelligence enables the ability to identify and track key threat actors, anticipate and inform decision-making and adjust response strategy to counter dangerous situations driven by political activism, social activism or critical events.

TAG Cyber: How do you deal with social media?

CONSTELLA: Social media is often overlooked as a significant threat vector to organizations, yet it requires automated, continuous digital risk protection across the full breadth of the internet. Social media platforms, both regional and global, play a significant role in executive impersonation, brand impersonation, disinformation and even employee safety. The reason social media is so important to monitor is because it provides a fertile ground for digital activism and influencer-driven pressure campaigns. It enables the creation of private spaces for organizing coordinated online or physical activities. To counter these threats, only continuous monitoring of a range of social media platforms enables organizations to recognize misinformation campaigns, reputation attacks or rallies at facilities, and then take pre-emptive action to minimize operational disruptions. However, these activities require more than the ability to track what's happening. They also necessitate the ability to monitor context and intent. In this scenario, multilingual capability and advanced AI become the keys to separating benign conversations from situations that demand corporate protection and response. Few businesses can track and analyze the global social media landscape on their own, especially across less visible platforms. However, understanding these threats is a next-level type of protection that should be on every corporation's must-have list, and we now feature it as part of our Dome platform.



CYBERWAR...THE DAY AFTER

GARY MCALUM

When I first entered the Air Force as a young second lieutenant in 1983, my first assignment was Castle Air Force Base in California. It was the primary base where they trained B-52 bomber and KC-135 tanker pilots. Those were the golden years of the Cold War, so the possibility of a nuclear conflict with the Soviet Union wasn't out of the realm of possibility. In that very same year, I gathered together one Sunday with several of my Air Force colleagues and watched the movie "The Day After." It was a very dark movie that was based on a fictional war between NATO forces and Warsaw Pact countries that rapidly escalated into a full-scale nuclear exchange between the United States and the Soviet Union. As you can imagine, it was filled with graphic, inconceivable consequences of such a war. I had a hard time sleeping for a while after watching it.

The geopolitical context for that movie I watched nearly 40 years ago feels a lot like what is happening today in Ukraine. And not just in Ukraine—in the South China Sea, in the Middle East and in North Korea. There are many flashpoint scenarios that could lead to nation state conflict on a scale we have not seen before. Recently in Ukraine, we've seen the unprecedented use of advanced hypersonic weapons by Russia even as Vladmir Putin raised the alert level of his nuclear forces. And North Korean dictator Kim Jong-un recently resumed testing of intercontinental ballistic missiles (ICBMs). We are living in precarious times indeed.

Many observers believe that in the next major conflict, cyberwarfare will be a key capability employed by our adversary at a level of scale and intensity we have not seen before. It's something that our military planners worry about. There are also some people who believe that the use of cyberwarfare capabilities by our potential adversaries will be limited—surgically precise and easily controlled. I am not one of those. In fact, I happen to believe the cyber component will create devastating impacts across our nation, impacting not just military systems but many critical infrastructures and daily conveniences we take for granted.

"Many observers believe that in the next major conflict, cyber warfare will be a key capability employed by our adversary at a level of scale and intensity we have not seen before. It's something that our military planners worry about."

As a former military cyber officer and private sector chief security officer, I have spent many years fighting the cyber fight and planning for worst-case scenarios. The very nature of cyberattacks is unpredictability, but here's what I think a nation state cyber conflict will look like.

While the initial event will likely involve military or warfighting systems, the cyber component will rapidly come into play. In a true nation state head-to-head confrontation that quickly devolves into significant military kinetic actions, I believe the cycle of escalation will increase rapidly and the cyber aspect will become much more visible. What will that look like in a major conflict? Planes will be shot down, ships blown up, communication and navigation satellites attacked with anti-satellite weapons and human life will be lost at a pace and scale we haven't seen since WWII. And cyberattacks will be widespread and devastating.

As any military strategist would argue, we can't know exactly how a true cyberwar will play out because there are scenarios ranging from low-end, inconvenient attacks all the way to the worst-case scenario of unconstrained cyberwarfare. No one knows what that looks like, but I think there are likely three simultaneous or overlapping scripts that we can expect to deal with. Remember, on the spectrum of possibilities, I'm talking about a far-right scenario where a sophisticated nation state adversary unleashes full cyber power, most likely in conjunction with traditional military kinetic capabilities. It's a horrible prospect to contemplate, but ignoring the possibility is dangerous.

1. DESTRUCTIVE MALWARE

Destructive malware will be widespread and targeted against military and civilian support systems, government organizations, financial systems and various critical infrastructures. Imagine a Sony Pictures scenario involving large financial institutions, our power infrastructure, and even logistics and transportation systems. It took months for Sony Pictures to fully recover. Can you picture banks or the market being down for just a few days, let alone weeks? And we've seen indications of this destructive aspect playing out in recent times.

It was less than five years ago that Russia unleashed NotPetya, a cyberattack targeting Ukrainian power, transportation and financial systems in an attempt to further destabilize the country. But rather than being the cyber equivalent of a precision smart bomb, NotPetya spread rapidly across the globe. That was a relatively unsophisticated attack compared to what a true sophisticated, destructive attack could do if fully unleashed. As of this writing, data wiping malware has already been discovered in Ukraine. So far, researchers have detected new destructive malware—HermeticWiper—on machines in Ukraine and nearby countries Latvia and Lithuania. The wiper abuses legitimate drivers from EaseUS Partition Master software to corrupt data.

2. SUSTAINED DISRUPTION OF SERVICES

Besides destructive attacks, we will have to deal with widespread and sustained disruption of services that we use on a daily basis. But isn't a distributed denial of service (DDoS) attack easily dealt with? Maybe not. Just last year, the New Zealand Stock exchange experienced a devastating DDoS attack

"There are also some people who believe that the use of cyber warfare capabilities by our potential adversaries will be limited—surgically precise and easily controlled. I am not one of those."

perpetrated by actors demanding a large sum of virtual currency in what became a "ransom denial of service attack" situation. Despite their best efforts to restore and sustain services, exchange trading at NZX was stopped for four days, with "only intermittent periods of availability," according to a government review. DDoS attacks are not new, and dealing with them should be relatively straightforward. But they have evolved and are easy to execute compared to more sophisticated attacks thanks to the explosive growth of internet-connected devices.

Disruptive attacks can also take the form of widespread delivery of ransomware. Think Colonial Pipeline. We can expect the Colonial Pipeline scenario to play out over and over across many industries and sectors should we be in a major military conflict. And don't forget the WannaCry ransomware virus back in 2017. WannaCry rampaged across the internet, attacking computers in 150 countries, causing massive productivity losses as businesses, hospitals and government organizations were forced to rebuild systems from scratch. Ultimately, hundreds of thousands of computers worldwide were affected. Just try to imagine multiple WannaCry viruses unleashed against the digital community. Any sophisticated, nation state actor will certainly use the DDoS and ransomware arrows in its quiver and do it at scale. Imagine the disruption of ATM functions or 911 phone operations or gas station operations or medical services for days and weeks on end.

While the disruptive effects of widespread and sustained DDoS and ransomware attacks are staggering to consider, there is one other aspect of a cyberwar that will likely come into the play, and it doesn't necessarily fit the context of cyberattacks we've been considering. The vulnerability of the world's transoceanic undersea cable infrastructure is amazingly underestimated, but definitely top of mind for military planners and our potential adversaries.

According to a 2021 article by the Center for Strategic and International Studies (CSIS), these major cable routes are sometimes described as the "world's information super-highways" and they carry over 95 percent of international data. In comparison with satellites, subsea cables provide high capacity, cost-effective and reliable connections that are critical for our daily lives. There are more than 400 active cables worldwide covering 1.3 million kilometers (half a million miles). Undersea cables make instant communications possible, transporting the vast majority of the data and voice traffic that crosses international boundaries. They also form the backbone of the global economy—roughly $10 trillion in financial transactions are transmitted via these cables each day.

While regional availability of the internet might continue to be accessible if international cables were cut, many critical services rely on data centers that are overseas, particularly the big tech companies based in the U.S. that dominate the web. A company's data may be housed in a data center located just down the road, but the business application that processes it may be running on a server on another continent. I have personal experience from my military days in dealing with a major communications outage caused by a fishing trawler dragging an anchor across a major undersea cable route. (At least that was the official explanation that was offered.) It made me realize that the potential implications for cyberwar are staggering, and the global undersea infrastructure would be a major target.

3. ZERO DAY EXPLOITS

Perhaps the most concerning characteristic of a worst-case cyberwar will be the unconstrainted use of zero day exploits creating both destructive effects as well as mass confusion. Think Stuxnet multiple times over. In that case, it was a very sophisticated worm exploit leveraging multiple unknown vulnerabilities in the Microsoft operating system to successfully target SCADA systems supporting Iran's nuclear program, specifically the gas centrifuges used for separating nuclear material. Stuxnet was able to stealthily change the physical performance of the centrifuge system while not allowing the monitoring system to report the anomalies that were injected into the processing. By the time lab personnel discovered the issues, about one fifth of Iran's nuclear centrifuges had been destroyed.

There's no doubt the world's cyber players are stockpiling zero day vulnerabilities and developing sophisticated exploits. If it comes to the worst-case scenario, the U.S. will have to deal with many such complex cyber events. Try to imagine, for example, what would happen if the nation's air traffic control system were compromised in such a way that controllers could not trust what they were seeing on their displays. And then imagine that the same thing happened in power distribution facilities, or water processing plants, or hydro-electric facilities and so on. The possibilities are endless and terrifying.

Some may argue that we've already been involved in a cyber conflict, and there certainly have been plenty of examples of limited cyberwar-like events. I think back to 2007 and the infamous "Web War I" Russian attacks against websites in Estonia, including its parliament, banks and government agencies. Most of the attacks that had any influence on the general population were good old-fashioned DDoS attacks, ranging from single individuals using various methods like ping floods to bigger botnet attacks. During my last military assignment, I recall meeting a senior Estonian official who told me that the attacks themselves were disruptive but not catastrophic. However, he went on to say that the biggest impact was the "loss of confidence in the government" among the people. Ultimately, that very result—a permanent loss of confidence in our government's ability to protect us—could be the lasting effect after a major conflict involving unconstrained cyberwar. And that might spawn a world not so different from the one I found so depressing in "The Day After."

IS THE GOVERNMENT'S VERSION OF ALL IN THE FAMILY A REALITY SHOW?

DAVID HECHLER

The **Aspen Cyber Summit** focused on the federal government's need to work collaboratively with the private sector in order to protect the nation's critical infrastructure. It was called "Exploring Collective Defense in a Digital World," and the emphasis throughout the two days was most decidedly on "collective." It could have been called "We're All In This Together."

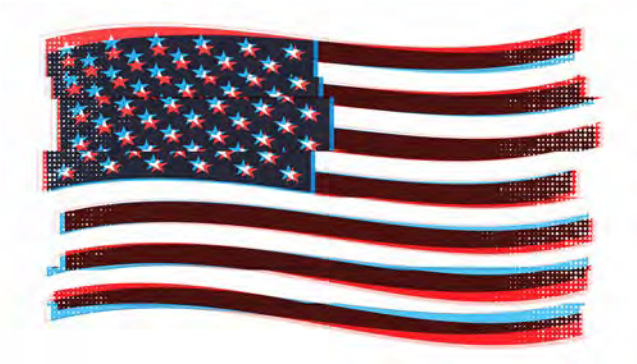
But just a few weeks earlier, Josephine Wollf, an assistant professor of cybersecurity policy at Tuft University's Fletcher School of Law and Diplomacy, wrote an article that suggested government agencies had serious problems working with each other. Specifically, she noted serious tensions between the offensive and defensive sides of the government's house. As I prepared for the conference, I wondered whether any of this would come up.

THE NEW KID ON THE BLOCK

In **"CISA Can't Succeed in the Pentagon's Shadow,"** Wolff argued that the U.S. Department of Homeland Security has never been given enough power to properly defend the nation's critical infrastructure, which is what its Cybersecurity and Infrastructure Security Agency (CISA) was created to do. CISA actually has several important roles, including working with regional officials to help secure elections. But the main focus for this conference was its role in helping to protect U.S. critical infrastructure by working with the companies involved, about 85 percent of which are in civilian hands.

Since its inception in 2018, CISA has been overshadowed by the Department of Defense, Wolff wrote. The National Security Agency and U.S. Cyber Command are the real powers in charge, she said. The Biden administration has expressed a desire to "marshal a whole-of-nation fight to confront digital threats," Wollf noted. But to do so, she continued, "it needs to embolden CISA so that it can begin to compel businesses and critical infrastructure

At a recent conference, government officials seemed intent on showing that they could work effectively not just with the private sector, but also with each other.



operators to take the necessary steps that will actually protect the country's most vital systems and networks."

She suggested that one recent development might be a hopeful sign. In July, Jen Easterly was confirmed as CISA's director. Easterly is a former NSA official herself. She helped launch Cyber Command. So "it's possible to interpret her new position as a sign of just how far the two departments have come in finally being able to work together and how well established and respected the DHS cybersecurity operations finally are," Wollf wrote. It's also possible to view Easterly's selection as a sign that the military has achieved hegemony, she added, pointing out that the top cyber officials in the White House, Chris Inglis and Anne Neuberger, are also former NSA officials.

Easterly was the conference's first speaker. She spent much of her time reviewing her 10 weeks on the job. She had plenty to say about collaborating. The most eye-catching piece was the new group CISA established in August: the **Joint Cyber Defense Collective** (JCDC). The partners include all of the government's heavy hitters: DoD, NSA, Cyber Command, DOJ, FBI, and more. From industry they've lined up Amazon Web Services, AT&T, CrowdStrike, Google Cloud, Microsoft, et. al. No signs of any friction there.

Interestingly, her bookend as the day's last speaker was Rob Joyce. Joyce is the government's fourth leader in the cyber realm, and he has not only spent much of his career as an NSA official, he's the only one of the four who is there now. He heads its **Cybersecurity Directorate**. Earlier in his career there he led the offense. His new job mostly involves intelligence.

Between Easterly's **presentation** and Joyce's, lots of examples of partnerships were discussed. (I wrote about some of them here.) But there was also talk about the need for an offensive response to the onslaught of attacks. "We can't only play defense," said Kevin Mandia, CEO of FireEye. He wasn't alone in urging more from the government. One example that drew praise from many quarters was the clawing back of at least some of the ransom that Colonial Pipeline paid to regain control of its data. In this instance, the FBI rather than Cyber Command was credited for the accomplishment.

THE NSA TAKES THE STAGE

When Joyce finally took the stage (yes, most of the panelists were really there), he was joined by journalist and author Garrett Graff, who directs cyber initiatives for Aspen Digital. Graff's first question was about a warning the NSA had just released concerning VPN vulnerabilities. "This was a **document**," Joyce responded, "that talked about what you should have in consideration for securing your VPN. And it was done jointly with CISA. They are our deep partner these days. There's almost nothing we put out that we don't do jointly with CISA—often CISA, NSA, and FBI together."

There was more along these lines. For instance, Joyce said that NSA has stood up its own **Cybersecurity Collaboration Center** to build relationships with private industry. It lacks the scope of CISA's JCDC, but it is a notable development for an agency with a go-it-alone ethos. But Joyce was not there to discuss his agency's conversion to collaboration. The topic of the session was "The Next Generation of Threats," and Graff skillfully probed for answers.

During the first year of the Trump administration, Joyce served as cybersecurity coordinator on the National Security Council for about a year before the position was eliminated. Graff asked him what's changed four years later. "The idea that cyber crime has become a national security issue," Joyce replied. "That to me is a dramatic change. And you see the government utilizing all elements of our power to include the foreign intelligence team, the offensive cyber team in the efforts to work against ransomware."

So what are the country's top threats? Joyce listed ransomware as No. 1. No. 2 is disinformation, he said, which is both "a cybersecurity problem and a malign influence problem." After that comes the nation-state threat. "Russia, China, Iran, North Korea: they roll off so easy," he said, "because those are the big ones we always see doing very obnoxious things in cyberspace." And the last is critical infrastructure. It's an area that "we've always known and worried about," but in the last five years it's grown urgent to lock down "for our national security."

Rob Joyce heads the NSA's Cybersecurity Directorate.

"You are the author of what is probably the most famous line about nation-state cyber threats," Graff said. "Russia is a hurricane; China is climate change."

It's still true, Joyce said. Russia is a disruptive force, often seeking to tear down adversaries by disseminating misinformation and malign information. And they actively gather intelligence on both governments and critical infrastructure. All make them dangerous, he added.

"Scope and scale, China is off the charts," said Rob Joyce. Its number of cyber actors "dwarfs the rest of the globe combined."

China still looks like climate change to him. "Scope and scale," he said, "China is off the charts." Its number of cyber actors "dwarfs the rest of the globe combined," he observed. "You talked about the difference four or five years ago to today," he said to Graff. "The difference I see is we respected them less. It was always broad, loud and noisy." But what they're finding, he went on, is that based on those numbers, the elite members of that group "really are elite." That makes them a sophisticated adversary.

The required response? Understand, disrupt and find ways to push back, Joyce said. "Defense is really important," he acknowledged. "But you also have to work to disrupt." The strategy is "continuous engagement," he said. "We've got to put sand and friction in their operations so they don't just get free shots on goal."

When people hear terms like "continuous engagement," he went on, "they think offensive cyber. It is," he said, "but I would say that the releases we've done jointly with CISA and FBI about the **N-day vulnerabilities** that those [adversary] teams like to use, that knocks them back just as much, and is just as important." As is working with the international community to establish "the expectation that these things won't be tolerated," he added.

What about Bitcoin, Graff asked. Is ransomware a cryptocurrency problem as much as a criminal problem? "Certainly without profit there is no ransomware problem," Joyce agreed. And crypto is the mechanism. But he called it both "a benefit and a liability." The transactions can be watched. "They're all very public," he said. "The question is, can you de-anonymize and connect them?" That's the challenge.

The other big challenge is **quantum-resistant cryptography**. When quantum computing arrives, unless they're prepared with cryptography that can withstand it, security will quickly dissolve. Confidentiality

algorithms, encryption algorithms, and authentication protocols will all be vulnerable, Joyce said. Now is the time to plan, he explained. That's their Y2K problem, but "orders of magnitude bigger." Asked how it's coming along, Joyce said "I'm feeling really good." For the classified networks, "we already have the protocols and the encryption technology," he said. And they're working with NIST to select commercial standards. "After you have all those things," he said, "it's the retrofit—it's the get it into everything and build it backwards."

THE BOTTOM LINE

So what are we to make of Wollf's concerns that CISA has been minimized? And if she had a point, were the conference presentations reassuring? To some extent, I think they were.

Even if the conference primed the pump for partnership, it does say something that so many individuals, including speakers from the private sector, spoke about the need for collaboration. Likewise, the decision by CISA and the NSA to create organizations designed to facilitate more effective cooperation between the public and private sectors—and in CISA's case, between government agencies as well—doesn't guarantee these will yield results. But it proves it wasn't just talk.

As for the way the government balances the two sides of its house, it's no secret that the offense in cyberspace has long outstripped the defense. And that's not going to change just because people talk a good game. It's also true that the offense is always going to get more credit (when its activities are made public). But if there was ever going to be a time to recognize that the country needs both sides functioning effectively, this is it.

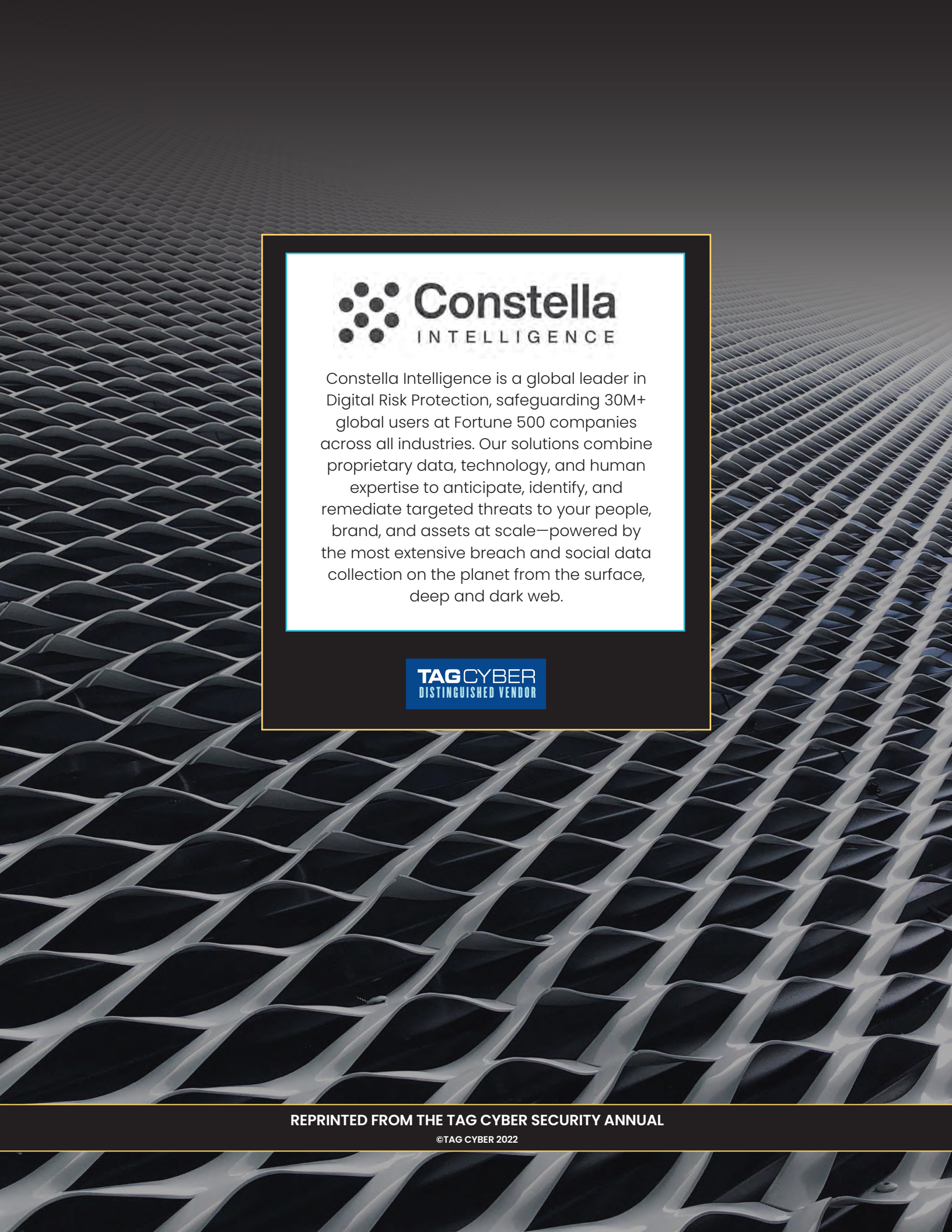
I think it does make a difference that Easterly made a name for herself at the NSA. And she has decades of high-level, relevant government experience. But what may be even more important is that defense suddenly seems top of mind. The country may never have appeared more visibly vulnerable.

The public heard about SolarWinds, and it sounded bad. But it was hard for a lay audience to understand what had happened. And then it only seemed to be about spying. Colonial Pipeline was very different. It was the infrastructure. And there were tangible results. Long lines at gas stations were on the evening news. All of those scattered ransomware attacks suddenly hit home in a big way. And they have not abated.

Where was the government?

At the conference, Rob Joyce talked about getting "left of theft." We need to be able to prevent these attacks, he said. "We really don't want the government, or any institution, to be really good at incident response. We've got to get ahead of that."

It's been a humbling time. The president of the United States had a talk with the president of Russia and told him the attacks had to stop. But they haven't. The talk about cooperation at the Aspen Cyber Summit didn't feel staged to me. It seemed to come from a bit of humility and a sense of necessity.



Constella INTELLIGENCE

Constella Intelligence is a global leader in Digital Risk Protection, safeguarding 30M+ global users at Fortune 500 companies across all industries. Our solutions combine proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your people, brand, and assets at scale—powered by the most extensive breach and social data collection on the planet from the surface, deep and dark web.

TAG CYBER DISTINGUISHED VENDOR

REPRINTED FROM THE TAG CYBER SECURITY ANNUAL