Cyber Risk
Director Network
August 2020

CRDN
VIEWPOINTS

Emerging cyber risks

In the second of three virtual sessions, members of the Cyber Risk Director Network met on July 1, 2020, to explore threats that are incipient, already developing, or possible given existing technology (but may not yet have become pervasive). Members and experts discussed the nature of these emerging cyber risks, actions that boards and companies can take now to mitigate them, and how anticipation of these risks might alter longer-term company strategies.

Members were joined by Chris Hoofnagle, Professor and Faculty Director at the Berkeley Center for Law & Technology, University of California, Berkeley; Angela McKay, Director, Emerging Threats and Risk Mitigation and Prevention at Google; Bill Phelps, Executive Vice President, Booz Allen Hamilton; Renee Rakowski and Jenny Vandrovec, Commercial Disinformation Advisory Practice leads at Booz Allen Hamilton; Kevin Richards, Executive Vice President, Booz Allen Hamilton; Katie Wilks, Principal, at Booz Allen Hamilton; Phyllis Sumner, Partner and Chief Privacy Officer, King & Spalding; and Steven Weber, Professor and Faculty Director of the Center for Long-Term Cybersecurity at the University of California, Berkeley. *For biographies of the guests, see Appendix 1 (page 14). For a list of meeting participants, see Appendix 2 (page 15).*

Discussion centered on three main topics:

- **The spread of disinformation**
- **Attacks on information integrity**
- **Quantum technologies**

The spread of disinformation

The intentional promulgation of false or misleading information to deceive individuals; social, political, or business groups; or organizations—already a widespread problem—is rapidly becoming a systemic issue, spurred in particular by the growth of social media. A director argued, *"the scope and scale of this is beyond all expectations."* Disinformation can come from nation states, criminals, or other groups with political or commercial aims; it can be spread by activists, disgruntled employees, or competitors seeking to gain an edge. These attacks are frequently aggravated by unwitting participants who spread disinformation, often through non-curated sources, amplifying their impact. A director remarked that *"untruths of this kind will go a much greater distance than a thoughtful, critically written piece."* Ms. Vandrovec agreed:

"The information is seeded, and the originator gets others to do the work: everyday individuals spread the attack."

Today's disinformation attacks typically unfold along several vectors:

- **Deep fakes** use artificial intelligence (AI) technology to alter images, recordings, or videos so that one person, or even a synthesized voice or image, is substituted for another—for example, putting funny words in the mouth of a celebrity. But the technology can also be used for deliberate deception, e.g. a telephone or video order to a bank to transfer money into a criminal's account. The technology is rapidly becoming highly sophisticated and producing ever-more convincing fakes.[1]

  "The sophisticated tools that are emerging," however, aren't the only serious threats, and simpler forms of deep fakes can be produced by near-amateurs, Ms. Vandrovec noted. She gave the example of *"an executive working from home. How easy is it for a bad actor to have a very grainy video, and to say it's a leaked video of a webinar?"* Particularly in the current work-from-home environment, *"the graininess gives some type of credibility. Now imagine,"* Ms. Vandrovec continued, "*a world where this kind of attack is not just put out there to try to damage reputations; what if it's now the new ransomware? What if the target is not just a data file that's part of your assets but rather bad actors having damaging evidence of you saying something that affects your entire company and your stakeholders?"*

- **The 24-hour time bomb** is a *"quick, intentional, acute attack"* that usually appears in mainstream sources, Ms. Vandrovec said. *"You see the consequence within a very short period of time."* A well-known case is the false rumor that the CEO of Ethereum had died in a car crash. The company's value briefly dropped by about $4 billion.[2] Since then, Ms. Vandrovec commented, such attacks have become more sophisticated and convincing through the introduction of audio and visual elements, such as an audio recording impersonating a CEO.

- **The slow decay of truth** is *"the most damaging"* disinformation attack, and a *"blind spot"* for most companies, said Ms. Vandrovec. *"Individuals and groups will seed little bits of inaccurate data in larger bodies of factual material. The intent is to make the falsified information less obvious as a standout and instead make it part of a cohesive narrative that is largely true. People then start spreading it and putting their own message around it."* Ms. Vandrovec offered the example of arson attacks on 5G mobile towers, spurred by fears that the technology posed health risks. *"While that was a 24-hour time bomb—an immediate visual image that people could internalize—it was started long before by foreign states that wanted to catch up with the rest of the world in 5G technology. They started seeding little bits of disinformation that 5G could cause infertility or cancer. And you'd read these things in the context of other data that was legitimate, or these articles would come from falsified groups that sound legitimate. It starts traveling through blogs and online comments, and the* *original source of the information has long since been removed from the conversation. Now COVID enters; what a perfect way to amplify these doubts."*

Why are disinformation attacks a top emerging risk?

Disinformation attacks can be quick, easy ways to create serious doubt and harm that may be difficult or even impossible to reverse. And while many such attacks are perpetrated by organized malicious actors, they can also be carried out by insiders—a potential threat that could intensify amidst the uncertainty of the COVID-19 pandemic.

Disinformation attacks present bad actors with many advantages:

- **Disinformation can inject doubt and cause financial or reputational harm.** Attackers can actively spread disinformation that leads investors to short a company's stock; competitors or others may make false claims to devalue a brand, causing reputational damage. *"Attackers—including activists or opportunists—inject doubt, the stock price comes down, another organization can pick up the stock cheaply and be the 'savior,'"* Ms. Vandrovec said. Disinformation can also cause broader harm. For example, a bank depends on the trust of its customers, and disinformation can erode that trust. One bank director said, *"We need to keep enough cash on hand so that currency is always available in ATMs. The last thing you want is disinformation or misinformation getting out there that there's a run on the bank—that's potential chaos."*

- **Damage from disinformation can be hard to reverse.** Guests and directors commented on the difficulty of countering or correcting disinformation. A director said, *"Once misinformation or disinformation is out there, you can't get it back. You're racing against something that you can't catch once it's out of the barn. If you haven't told your story first, you can't tell it second; you simply can't."* Another director said, *"Disinformation is critical, not just for the corporation or for directors but as a country. I'm not sure why we tend to fall prey; is it something we've come to expect so we don't question it carefully?"* Without good models of how disinformation actually moves through markets and societies to affect perceptions, it can be hard for security professionals to prevent and respond to attacks.

- **The potential for disinformation to create insider threats may increase in the time of COVID-19.** *"For so many employees,"* a director noted, *"working remotely is a vulnerable time psychologically. They may be vulnerable to disinformation."* Add to that employees' worries about how to properly protect their health and whether their jobs are secure, and the director wondered, given increasing workforce anxiety and uncertainty, *"is there is an insider threat component that an adversary could take advantage of?"* Another director noted that trust in official information can quickly erode and *"the social fabric can be weakened. We need to be careful that physical distance doesn't create social distance—that the social fabric that connects people to the culture and the daily rhythms of the company isn't weakened."*

How can leaders prevent or mitigate disinformation?

The frequency of disinformation attacks on companies is growing, Ms. Vandrovec said. Leaders need to focus on disinformation trends and strategize about how to get ahead of disinformation campaigns. Ms. Vandrovec advised taking the time to manage information in advance rather than being forced into crisis-management mode:

- **Know which intangible assets matter most to your stakeholders.** It's crucial to *"understand who is interacting with your organization,"* said Ms. Vandrovec*. "Know what's motivating them, what's scaring them."* But, she added, it's important to be aware that, often, attacks don't happen *"within your four walls or even directly on your brand—it might be two or three nodes out."* Getting a good sense of your ecosystem, she said, means *"looking at the foreshadows or signals"* and deciding what is most important to stakeholders—a reputation for putting customers first, for example*. "It may not be the assets or intangibles your executives consider most important. Executives often assess the potential risks from actual events -- a cyberattack, product defects, or failed mergers – but forget that the perception of an issue can be equally powerful. Perceived vulnerabilities such as concerns about executive integrity or product safety, if activated en masse, can shift reputation and sales."*

- **Look for smoke signals and subtle signs of concern or discontent.** This can help buy time to respond effectively to attacks. Ms. Vandrovec reiterated the importance of looking beyond the organization's *"four walls"* and being on alert in order to *"give yourself enough time to respond. It's knowing that a crisis could occur and expanding that window of opportunity out of which you can see a probable action, or a flame that could start to ignite, and when it starts to get out of control."*

- **Do impact assessments.** *"Measure what you're seeing,"* said Ms. Vandrovec, including *"how social media attacks are affecting consumer confidence."* Thinking through the application of that data and responding appropriately requires an awareness that not all alerts *"will translate into operational, financial, or reputational damage. It might be that the peaks are occurring with stakeholders who are outside the scope of what drives your business,"* she noted. To respond to threats appropriately, companies must map the data they collect to their strategic priorities.

- **Reassess organizational structure and assign ownership of the risk.** Ms. Vandrovec stressed that *"disinformation can cut across the entire business, so the solution involves the entire business. Reassessing, looking at potential silos; the functions involved—do you have the right business intelligence? The right threat intelligence? Do you have the right governance prompts for alerts? The right feedback so that groups that are getting hit with information attacks can learn from them and relay the news to the rest of the business? There's no gold standard; everyone is learning."* Since modern disinformation attacks are still relatively new, Mr. Richards said, many companies *"don't know who owns this risk."*

Determining this is crucial because, he added *"this isn't just a technical problem, although there's technology that can be used to address it."*

- **Solving the problem may require private-sector coordination.** A director argued that the private sector will need to coordinate in order to address these issues, as governments will not act on their own. *"In the 19th century, we had a Wild West of fake stock certificates, fake land titles, and so on, and over time we built up an industry of notaries, title companies, and registries, as well as legislation, and eventually that kind of thing has been squeezed out. We're in the Wild West right now with disinformation. It's not a solution to just wait—we have to go on the attack."* Ms. Vandrovec pointed to some *"evolving regulations"* like the European Commission's Code of Practice on Disinformation, noting that even TikTok has now signed on. The code's adherents agree "to a set of voluntary steps aimed at combating the spread of damaging fakes and falsehoods online."[3] Ms. Vandrovec added, however, that "*the bad actors have an unparalleled degree of creativity"* and can easily *"get through the loopholes— and therefore much more collaboration and coordination is needed."*

Attacks on information integrity

Data integrity is central to information security and companies must safeguard their data to protect against errors, alterations, and any possible damage from manipulation, in addition to the more common concerns about cybersecurity data breaches in which access to and theft of data are the primary threats.

Instead of stealing information or locking it up for ransom, information integrity attackers modify it in place, rendering critical information unreliable, unusable, or insidiously inaccurate in ways that have downstream impact. These attacks are on the rise across all phases of data collection, storage, use and destruction. Ms. McKay explained that, as organizations have better protected themselves from breaches and increased their overall resilience, attackers are moving toward less defended areas. Information integrity attacks are particularly appealing, she said, because they involve small but consequential changes that are difficult to detect.

Ms. McKay described several vectors that malicious actors use to compromise information integrity:

- **Data creation, storage, processing, and updates.** Information integrity attackers can target data, algorithms, or software, said Ms. McKay, and corrupted data need not reside within a company's servers. She recalled an early case involving the hack of the Associated Press Twitter handle. In 2013, the official Twitter account of the AP tweeted that there had been two explosions in the White House and that President Barack Obama had been injured. But the AP had not actually initiated the tweet, and the Syrian Electronic Army later claimed credit for it. The AP security team quickly alerted users to the attack, but investors had already panicked, and the Dow Jones Industrial Average plunged more than 140 points.[4]

- **The software supply chain.** Information integrity issues are also seen in the software supply chain. Ms. McKay noted that developers, who frequently use open source libraries, may import corrupted code which then proliferates over the entire ecosystem.
- **Machine learning (ML) environments that trick systems or the people managing them.** Data-integrity attacks can trick or manipulate ML systems into making classification errors or bad decisions. By altering the data, such attacks can also confound the people managing ML systems, thus creating a whole new level of risk, according to Ms. McKay.
- **Analytics and ML attacks on training data or algorithms.** It is very difficult to detect whether training data or algorithms have been corrupted. Ms. McKay said that researchers and data scientists who are working on detecting manipulation of AI and ML systems are focusing on explainability -- the explanation of the internal mechanics of a machine or deep learning system in order -to understand how algorithms reach conclusions. 'Explainable AI' aims to make AI more accountable by uncovering bias, debugging learning models, and detecting adversarial activity that could distort predictions or decisions.[5] The field is very new, however, and Ms. McKay noted that the mitigations and risk management techniques currently available are as yet inadequate to the task.

Data-driven learning systems are brittle and highly vulnerable to manipulation

A director elaborated on information integrity risks in machine learning. *"By manipulating input data to an ML algorithm that's already been trained, you can get it to misclassify normal things: change a stop sign to a 60mph sign, for example. And it's worse than that, because we're discovering that ML algorithms that recognize objects and images—this is a Labrador dog, this is a school bus, this is a turtle, etc.,—are not doing this in the way that you or I would. A recent MIT paper described an algorithm that decided whether there was an airplane in a particular image by looking at whether one pixel was a certain gray color. In all the images it was trained and tested on, that was a successful strategy for recognizing airplanes. The algorithms will use any statistical regularity in the training data, regardless of whether it makes sense to you or me. This means you can get these things to misclassify extremely easily. You don't have to do lots of clever manipulation of images, you can just put a gray pixel there and the algorithm will think it's an airplane.*

Data-driven learning systems are brittle and highly vulnerable to manipulation

"We have also shown that robot systems trained via reinforcement learning—for example, to carry out complicated tasks like playing soccer—can be spoofed even without fake data. It's enough to make other parts of the environment behave in unexpected ways. You can just get the goalkeeper to fall over, and then the soccer playing robot who's trying to score a goal doesn't know what to do because he's never seen a goalkeeper fall over before, and just falls over himself.

This suggests that data-driven learning systems are far more vulnerable than we think, because they are not developing any kind of robust understanding of images, or of the video, or of the application form of the insurance applicant or the credit applicant; they're often relying on spurious regularities."

- **Success motivates further attacks:** Ms. McKay remarked on a reinforcing cycle in information integrity attacks: malicious actors recognize that their incursions are hard to detect or trace, and this emboldens them to carry out further attacks. A director added, *"I'm not sure whether AI/ML manipulation will be a major attack mode … but I am sure that the malfeasance sector is paying attention and trying to figure out how to take advantage of it. So I would strongly recommend not using black box recognizers for anything that is critical—decisions on behalf of an individual such as credit, medical, etc.—anything that impacts the bottom line if it involves data that could affect people."*

Why is information integrity high on the list of emerging risks?

Information integrity attacks can be even more dangerous than data theft. Data manipulation aims to breed distrust and to compromise the integrity of a specific target. And while information integrity attacks, like data theft, can be exploited for profit, the motivations behind these attacks are more diverse and unpredictable. Participants focused on several reasons these attacks are on the list of emerging risks:

- **Information integrity challenges are insidious and hard to detect compared to other risks.** Ms. McKay explained that a major challenge of data integrity attacks is that they are very hard to detect; sometimes the victims of such attacks aren't even aware that they have occurred. She illustrated this by contrasting for instance, confidentiality breaches with information corruption attacks. In the case of a confidentiality breach, a company might lose data, but however serious the loss, will generally be aware of it and overall operations will not typically be disrupted. Comparing a data corruption attack to a denial-of-service attack that compromises online availability, she noted that the latter might disrupt some operations, but that the company would be aware of it. In the case of outright data theft, IT professionals can often see evidence because they have tools that monitor the movement of data. But with information integrity attacks, data does not move, so the impact may not be detected until there is a reason to question the data.

- **The potential impact of data integrity attacks is high but not fully understood; mitigations are not yet well-established.** Ms. McKay described the impact of data integrity attacks as both insidious – causing a gradual erosion of data reliability – and extremely serious. She explained that the industry is still trying to come to grips with the wide range of possible consequences of these attacks for companies' operations, their brands, and the economy overall, adding that the available mitigations are inadequate to manage the risk.

How can leaders prevent or mitigate information integrity attacks?

Although a few tools are available for preventing or mitigating attacks, Ms. McKay said, they do not on their own meet the challenge. She suggested that companies should invest in research on practical methods to detect and combat this risk. There are mitigation steps companies should take:

- **Improve segmentation.** Ms. McKay advised companies to adopt strategies that complicate attackers' tasks and limit the overall impact of data integrity attacks. These include taking advantage of cloud computing and microservices to reduce large applications to smaller, self-contained component parts that can be managed by dedicated teams.
- **Apply ML and analytics to check for corruption in large data sets.** Even in the absence of intentional corruption, all large data sets have flaws and gaps. This makes it challenging to distinguish normal noise from intentional manipulation. In this case, new technologies may be sources of exposure and offer opportunities to mitigate risk. Ms. McKay remarked that, ironically, the application of ML and analytics is one avenue of mitigation, since these approaches can help uncover anomalies between data sets as well as identify and understand discrepancies among mirror images and backups.
- **Employ secondary systems to provide continuous validation as a safeguard.** Mr. Phelps noted that, *"as we become more and more dependent on AI/ML or robots—whether in cars or credit scoring, [there are] more and more situations where we're trusting a black box—we have to have second systems that provide continuous validation of that trust."*

Quantum technologies

Quantum technology applies the laws of quantum mechanics to create a new computing architecture that will revolutionize certain kinds of information processing and communications networks, imaging, cryptography, and simulation. Quantum computers and sensors for imaging use the quantum properties of subatomic particles (including quantum entanglement, quantum superposition, and quantum tunneling) to store and process information. These technologies may be able to find solutions to problems that have "almost infinitely many variables—a huge number of moving atoms, for example."[6] The calculation powers of a fully functional quantum computer would be orders of magnitude greater than the capabilities of existing computers, and could transform many fields, including materials science, engineering, chemistry, and medicine. Such a machine would almost certainly also be able to crack some standard encryption methods, a potentially significant risk in the hands of malicious actors.

Timeline for the development of quantum computing.

Many companies are working on quantum computing, and several universities and militaries are helping to fund research in a number of countries. Early prototypes do exist, and Dr. Hoofnagle thinks that a large quantum device is less than 10 years away. *"The technologies that create the underlying quantum effects are becoming cheaper and are even commercially available. The barriers to entry are lower,"* he said, adding that multiple technologies can maintain qubits (quantum bits, the fundamental object of information in quantum computing). In addition, noted Dr. Hoofnagle, *"there's a huge amount of money flowing in, both from the government and from the private sector … There's an enormous amount, for instance, from the Army research lab; also from the National Science Foundation. In China, there is at least $3 billion in funding from the state—and that doesn't include supplementary funding from huge Chinese companies, Baidu and the like—that have committed to massive investments."*

Dr. Hoofnagle foresees quantum computing capabilities being available on a cloud basis for the most part, and rarely inside most enterprises, noting that *"they are extremely sensitive. Most require super-cooling, so they need helium rigs to keep them cold."* While most companies would be unable to provide the physical environment necessary for quantum computers, large cloud providers would more likely be able to manage a challenging engineering problem like keeping quantum computers close to the absolute zero temperature they require. And "whoever makes the engineering breakthrough to build one of these devices," Dr. Hoofnagle explained, "*very well could be in the private sector—we shouldn't assume it'll be a government. It could be IBM, or Microsoft, or Google, and they will want to keep their engineering secrets secret. There's no better way to do that than to sell this through the cloud as a service."*

Hurdles and challenges remain, including a lack of fundamental agreement on materials and practical approaches to assembly of quantum computers, as well as the software tools that will be needed to take advantage of quantum architectures. Such challenges, together with the need to keep the machines at extremely low temperatures, present barriers to scaling quantum systems. Finally, assessing the efficacy of early-stage prototypes is difficult. Nevertheless, Dr. Hoofnagle and Dr. Weber believe that the basic science problems are largely solved; what remains are engineering issues that are complex but well understood.

Potential risks to companies

While quantum technology could pose risks to certain types of encryption, Dr. Hoofnagle does not believe that this will be the most important area of focus for companies that develop quantum computers, because the technology offers greater opportunities in other areas. Nonetheless, it has the potential for several types of security risks. In addition, quantum is a disruptive technology that may become a significant competitive challenge to companies in the industries it transforms. CRDN participants discussed several areas of potential risk quantum computing may pose:

- **Private developers of quantum computers are unlikely to pose significant confidentiality or data-integrity risks.** *"So much talk of quantum computing surrounds attacks on confidentiality and integrity,"* Dr. Hoofnagle remarked. *"But there's a path dependency to this. The first quantum algorithms were focused on factoring and search, and so people immediately realized: Well, if this quantum factoring algorithm really works, then RSA encryption is toast. That fact has steered the debate. But these devices will be far more useful for other purposes, and companies will make far more money doing chemistry and drug development than cracking encryption keys. So that's the bright side: that we're on the precipice of new research frontiers, particularly in materials science and chemistry, that will be far more exciting than attacks on confidentiality."*
- **Quantum attacks will focus on particular vulnerabilities.** In the event that they develop a quantum computer, Dr. Hoofnagle does not believe that the *"Microsofts of the world"* have any real commercial interest in threatening the security of other companies. *"There's much more money to be made moving into drug discovery or other areas,"* he said. If, on the other hand, a company has IP that is of interest to foreign countries, those entities may be willing to use quantum devices to steal it. In any case, practical considerations pose obstacles to using quantum computing to break encryptions, he explained. *"Based on projections for today's quantum computers made by scientists at IBM and Google, the National Academies of Sciences, Engineering, and Medicine project that it could take 28 hours to crack a single RSA key if such a device were to be scaled to a very large size. If it takes a full day of computing resources to attack a single encryption key, then intelligence agencies and others out there will choose very carefully the keys they want to attack. They are more likely to devote their resources to attacking software signatures, password hashing, and … device attacks, because with that daylong investment of computing resources, you get more value from the attack."*
- **Corrupted software signatures could be a concern.** Dr. Hoofnagle believes that, rather than confidentiality issues, the more serious problem companies may face is compromise of software signatures, leading to the promulgation of corrupted software updates. *"Whether it's intelligence agencies or others pushing out updates in order to capture all information*

about users on a device—this is a much more likely attack and it's not discussed as much as things like credit card numbers."

- **Quantum is a massively disruptive technology and poses potential competitive risks.** These risks are particularly important for companies in the materials science, chemistry, and pharma sectors, and possibly financial services as well. If major private-sector companies like IBM or Google develop quantum technologies, they may become much bigger than the proverbial "800-pound gorilla" in markets they enter.

How companies can prepare for quantum technologies

Companies can take precautions, including evaluating company secrets and the best ways to safeguard them, adopting high standards for encryption technology and rethinking data retention policies:

- **Companies should critically evaluate their secrets.** Dr. Hoofnagle advised companies to think carefully about their secrets. Some companies could be targets of a quantum-driven nation-state attack. If, for example, a company has *"valuable IP of interest to the Chinese, a nation-state with a quantum computer could use it to try to make sense of your company's secrets,"* he said. Dr. Weber remarked that *"for the foreseeable future, you'll be dealing in a world of limited capabilities that will be used for high-value efforts,"* so directors should protect the company's crown jewels. However, Dr. Weber added, doing so *"may require a flip of perception: What are those high-value targets for attackers who want to move a variable in a direction that suits them?"* In deciding what those secrets are, keep in mind that reputational considerations are also important, Dr. Hoofnagle said: *"It turns out that in the world of WikiLeaks, the off-color remarks of a CEO in email or other uncontrolled environments are also dangerous."*
- **Quantum sensing will make physical secrets easier to detect.** Quantum sensing is a prerequisite to quantum computing: *"You have to get quantum sensing right to get quantum computers to actually work,"* explained Dr. Hoofnagle. The technology *"could be really important,"* he added, and is a central focus of military research in both the United States and China. Quantum sensing promises many new capabilities across a variety of fields, including detailed underground mapping and improved imaging capabilities even at long distances. Dr. Hoofnagle noted that some companies, particularly those in the natural resources space and extractive industries like oil or gas, should be aware that quantum sensing *"involves new forms of detection that will make it harder to keep secret, for example, what natural resources are in an oilfield. If your organization has secrets in the physical world, they'll get harder to protect against this type of inspection."*
- **Companies should adopt AES encryption, which is more resilient to quantum attacks.** RSA encryption will be vulnerable to quantum attacks, although the National Institute of Standards and Technology *"is working on post-quantum crypto systems that should be*

resilient against quantum, and we should be thinking about transitioning to those," Dr. Hoofnagle said. He added that Advanced Encryption Standard (AES), *"which we use to encrypt our hard drives and for other purposes, is still resilient."* AES supports various block lengths, including 128, 192, and 256 bits, which confer increasing degrees of protection. it is "immune to all known attacks" using nonquantum technology, making it "the gold standard of encryption."[7] AES-128, often used for storage security and disk encryption, *"will be secure against most attacks,"* and *"AES 256 is secure for thousands of years,"* Dr. Hoofnagle noted.

About this document

The Cyber Risk Director Network (CRDN) was founded to bring together business leaders and experts with a broad goal of enhancing national cybersecurity by strengthening board oversight of the largest US companies. The network is sponsored by King & Spalding, an international law firm with a substantial data privacy and security practice, and by Booz Allen Hamilton, a management and information technology consulting firm with deep cyber and industry expertise. Tapestry Networks organizes and leads the network.

ViewPoints is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting directors, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Appendix 1: Meeting guests

- Angela McKay: Director of Emerging Trends and Risk Mitigation and Prevention, Google
- Chris Hoofnagle: Faculty Director, Berkeley Center for Law & Technology, and Professor of Law and Information, University of California, Berkeley
- Renee Rakowski: Commercial Disinformation Advisory Practice Lead, Booz Allen Hamilton
- Jenny Vandrovec: Commercial Disinformation Advisory Practice Lead, Booz Allen Hamilton
- Steven Weber: Professor, University of California, Berkeley School of Information; Director of the Center for Long-Term Cybersecurity and Professor, Berkeley School of Information Science
- Katie Wilks: Principal, Booz Allen Hamilton

Appendix 2: Meeting participants

- Joan Amble: Zurich Insurance Group, Booz Allen Hamilton, Sirius XM
- Marianne Brown: Northrop Grumman, Akamai Technologies, VMWare
- Bill Easter: Concho Resources, Delta Air Lines, Grupo Aeroméxico
- Linda Gooden: ADP, General Motors, Home Depot
- Pat Gross: Liquidity Services, Perdoceo Education, Rosetta Stone
- Fritz Henderson: Marriott International
- Chris Inglis: FedEx, Huntington Bancshares
- Leslie Ireland: Citigroup
- Tom Killalea: Akamai Technologies, Capital One Financial
- Holly Keller Koeppel: AES, British American Tobacco
- Jane Holl Lute: Union Pacific, Marsh McLennan Companies
- Bill Phelps: Executive Vice President, Booz Allen Hamilton
- Kevin Richards: Executive Vice President, Booz Allen Hamilton
- Stuart Russell: Intact Financial
- Phyllis Sumner: Partner and Chief Privacy Officer, King & Spalding
- John Thompson: Norfolk Southern
- Lynn Vojvodich: Booking Holdings, Dell, Ford
- Sue Wagner: Apple, BlackRock, Swiss Re

Endnotes

[1] Martin Giles, "The GANfather: The Man Who's Given Machines The Gift of Imagination," *MIT Technology Review*, February 21, 2018.

[2] Jeff John Roberts, "Hoax Over 'Dead' Ethereum Founder Spurs $4 Billion Wipe Out," *Fortune*, June 26, 2017.

[3] Natasha Lomas, "TikTok Joins The EU's Code of Practice on Disinformation," *MSN,* June 22, 2020.

[4] Julianne Pepitone, "AP Hack Proves Twitter Has a Serious Cybersecurity Problem," *CNN,* April 23, 2013.

[5] Meet Gandhi, "What exactly is meant by explainability and interpretability of AI?" Analytics Vidhya, February 15, 2020

[6] Lars Tvede, "The Present And Future Of Quantum Computing Expansion," *Forbes*, July 14, 2020.

[7] Dave Wallen, "AES Encryption: A Closer Look at Advanced Encryption Standards," Spanning, May 26, 2020.