Verisk Perspectives

A Report by ISO Emerging Issues

The climate change challenges you need to know about

Cyber threat: Increasing connections, increasing danger

5G technology: Promises and perils on the horizon

Cannabis 2.0: The coming age of bioengineering

Verisk

Table of Contents

Introduction

Charting a Course Through Today's Emerging Risks 3

Climate Change

Arctic Warming Could Be Impacting the Jet Stream…and Bringing More Destructive Weather 6

Polar Vortex Splits Causing Major Disruptions 8

Sea Level Change: Examining Hot Spots and Their Potential Implications for Insurance and Society 10

Where Climate Change and Natech Risk Meet 14

Climate Change: Transition Risks 17

Cybersecurity

Power Utilities Face Emerging Cyber Threats 22

Cyber Risks Loom Large in an Interconnected World 25

Could NotPetya's Tail Be Growing? 28

Cybersecurity Needs a Quantum Leap 30

5G Technology

5G: New Opportunities and Risks 34

Complex 5G Rollout Comes with Radiation Risks 38

Could 5G Deployment Disrupt Weather Forecasting? 40

How 5G Can Send Drones to New Heights 42

Cannabis

How Bioengineering Could Reshape the Cannabis Industry 46

As Market for CBD Products Blooms, Questions Grow around Human Safety 49

About Verisk Business Units 52

Learn More about ISO Emerging Issues 53

ISO Emerging Issues Team 54

Charting a Course Through Today's Emerging Risks

Understanding risks is a journey, not a destination. Nowhere is this more obvious than in the world of emerging risk analysis where researchers seek to identify new risks and learn how old ones may evolve.

We believe such research can empower the insurance and risk management industries with actionable insights to both help mitigate potential risks and leverage product-building opportunities.

That's why Verisk is constantly investigating the potential future effects of various trends, such as technology, health, and environmental science. From climate change and evolving cyber threats to the promise and peril of 5G networks and cannabis's march to the mainstream, we're training our sights on the critical questions that could shape and reshape not just entire industries, but entire societies as well.

Verisk Perspectives provides you with insight into four topics that experts across our multiple companies have been following: climate change, cybersecurity, 5G technology, and cannabis.

Climate Change: Pairing sophisticated data and catastrophe modeling with environmental fact gathering, we explore pressing questions about our evolving climate crisis, including the climate's influence on the planet's jet streams and how rising seas may impact coastal flooding.

Cybersecurity: Global supply chains, once subject to physical disruption through weather or geopolitical events, are now increasingly vulnerable to virtual sabotage due to their reliance on a wide-ranging network of third-party business partners as well. How can insurers manage this interconnected business? And how will the cybersecurity industry react to the introduction of quantum computers, which may be able to crack today's most complicated encryption algorithms with ease?

5G Technology: Cellular carriers around the world are preparing to turn on 5G networks, tempting consumers and businesses alike with tales of blazing download speeds orders of magnitude faster than 4G and significant decreases in latency. So why could weather forecasting stand to be negatively impacted with the transition to 5G? Also, how can 5G's capabilities support the development of other critical technologies, such as drones?

Cannabis: As cannabis use may likely continue to increase across the United States, it is important to be cognizant of the risks that may coincide from a wide range of angles. For example, as the regulatory regime has become more permissive, researchers are facing an entirely new set of challenges around drug and pesticide interactions. But could bioengineering reduce these risks?

We certainly hope that by reading *Verisk Perspectives* you will not only gain valuable insight into these four topics but also see the value the Verisk family of companies brings to your business.

To learn more about these and other risks we research, I urge you to check out our ISO Emerging Issues website on ISOnet (ISOnet login required) and our Visualize content hub where you can sign up for weekly e-newsletters that can help you keep up with the evolving risks that may be facing your business.

Sincerely,

Mark Anquillare

Mark Anquillare
Chief Operating Officer
Verisk

Climate Change

6 Arctic Warming Could Be Impacting the Jet Stream…and Bringing More Destructive Weather

8 Polar Vortex Splits Causing Major Disruptions

10 Sea Level Change: Examining Hot Spots and Their Potential Implications for Insurance and Society

14 Where Climate Change and Natech Risk Meet

17 Climate Change: Transition Risks

Arctic Warming Could Be Impacting the Jet Stream…and Bringing More Destructive Weather

By: Judah Cohen, PhD

Climate change debates are partly driven by the complex interconnectedness of weather systems and how each component may or may not affect the other.

The potential changes emerging with jet streams serves as an example, where different sets of factors could be aligning to create tangible shifts in weather patterns with potentially serious consequences.

Gradients: A primer

Jet streams operate, in part, due to temperature differences between the poles and the equator, a margin known as a gradient. If the temperature difference between the equator and poles is high, then the gradient is strong. As that temperature gap closes, the gradient is then weakened. It's important to keep in mind that the speed of the jet stream is sensitive to the equator-to-pole temperature gradient.

However, the temperature difference between the poles and equator isn't the only gradient that may impact jet streams. There's also a gradient between the North Pole and the northern edges of the continents as well as between the equator and midlatitudes.

> "We could be faced with slower and more split jet streams and…more extreme weather."

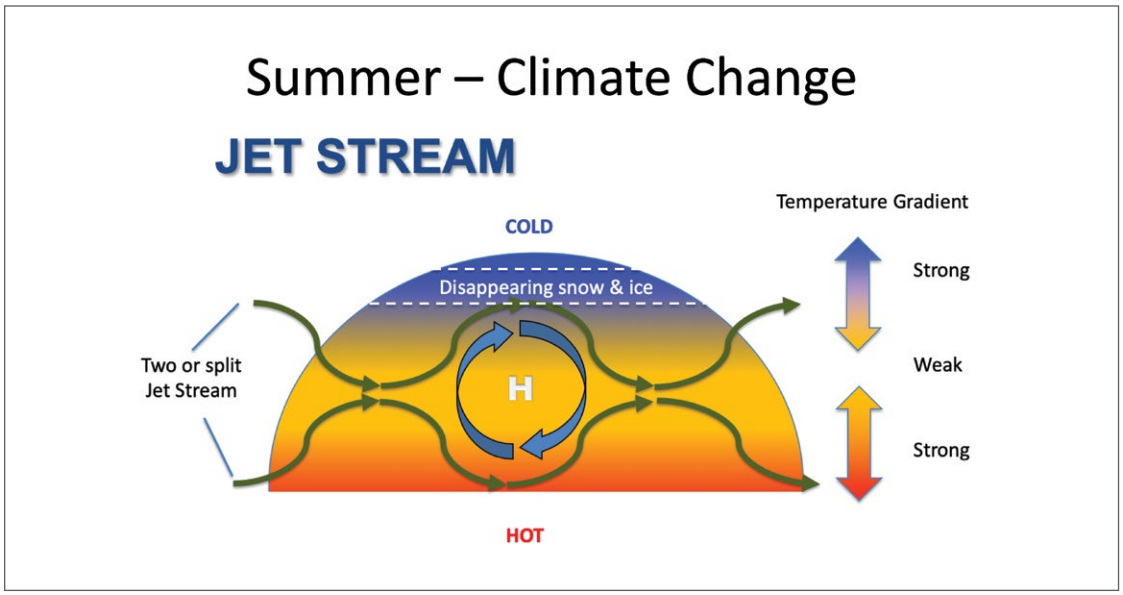
With temperatures increasing 2 to 3 times faster in the Arctic than the rest of the world, the gradient between the North Pole and equator is the most extreme instance of a weakening gradient.

In the summer, the North Pole/equator gradient has grown weaker. However, the gradient between the North Pole and the northern edges of the continents this time of year is strengthening. Why is this? The greatest warming is transpiring on this northern continental edge, more so than at the North Pole. Therefore, the temperature differential is increasing, strengthening the gradient. Additionally, since warming has been evenly spread across the equator and midlatitudes, there hasn't been a substantial change in gradient in this region.

What it means for global weather patterns

Ultimately, the strengthened gradient in the high latitudes, the weakened gradient from the North Pole to the equator, and the relatively unchanged gradient between the midlatitudes and equator could contribute to a split in jet streams during the summer—one to the north and the other to the south.

This split could allow weather systems to move more slowly across the Northern Hemisphere and could even cause weather systems to become trapped or stationary between the two or split jet streams, creating favorable conditions for these weather systems to strengthen and create more extreme weather.



Two regions of strong temperature gradients = two jet streams. In between the jet streams weather systems such as heat domes become trapped.

This precise scenario may have manifested itself, for example, through the record-shattering heat waves that engulfed Europe in the summer of 2019.

If the temperatures in the Arctic continue to stay at present levels, or even rise further, then we could be faced with slower and more split jet streams and the more extreme weather events that they carry in their wake.

Contributor
Judah Cohen PhD, is Director, Seasonal Forecasting, Atmospheric and Environmental Research (AER).

Polar Vortex Splits Causing Major Disruptions

By: Judah Cohen, PhD, and Peter Sousounis, PhD

Nothing says winter like holiday music, hot chocolate, and the full panoply of snow sports. The last decade, however, has introduced a new and very disruptive winter tradition: the polar vortex split.

In the last several years, these splits have barged into the winter routines of millions of people, bringing arctic temperatures and treacherous conditions. But what exactly is a polar vortex split, and why are we hearing about it more frequently?

What is the polar vortex?

The polar vortex is a fast-flowing stream or ribbon of air that circles the upper atmosphere above the North Pole during the winter months. When the vortex is strong, the surrounding winds flow fast and in a straight west-to-east direction. Conversely, when the vortex is weak, the surrounding winds slow down and may even reverse direction and become much more meandering in a south to north direction. During the most extreme polar vortex weakening, the single, or parent, vortex normally centered on the North Pole will split into two daughter vortices, one in each hemisphere. Often, when the polar vortex is strong, temperatures are mild in the midlatitudes across the eastern United States, Northern Europe, and Asia. But when the vortex is weak, temperatures tend to be cold across these same regions.

In addition to the weakened vortex contributing to arctic temperatures in midlatitude regions, the Arctic itself is subject to a sharp swing in weather in the opposite direction. Just like opening the refrigerator door allows warm kitchen air to displace cold air in the refrigerator, warm subtropical air rushes into the Arctic during a weakened or split vortex. In 2018, Boston was subjected to 93 mph winds, and upstate New York received 40 inches of snow from one powerful nor'easter. What was the temperature in the North Pole during this stretch? Temperatures were 45 degrees higher than average, reaching a balmy 35 degrees Fahrenheit.[1]

> "One disruption following a polar vortex split in 2019 cost the U.S. economy $5 billion."

This contrast is representative of the disruptions in weather patterns that a weakened polar vortex can lead to. The frigid temperatures brought by a weak vortex aren't simply an annoyance for those who dislike the cold, they can hammer the economy. One disruption following a polar vortex split in 2019 cost the U.S. economy $5 billion.[2] Costs incurred from this event included property damage as well as a significant loss of income due to arctic conditions paralyzing industry for multiple days.

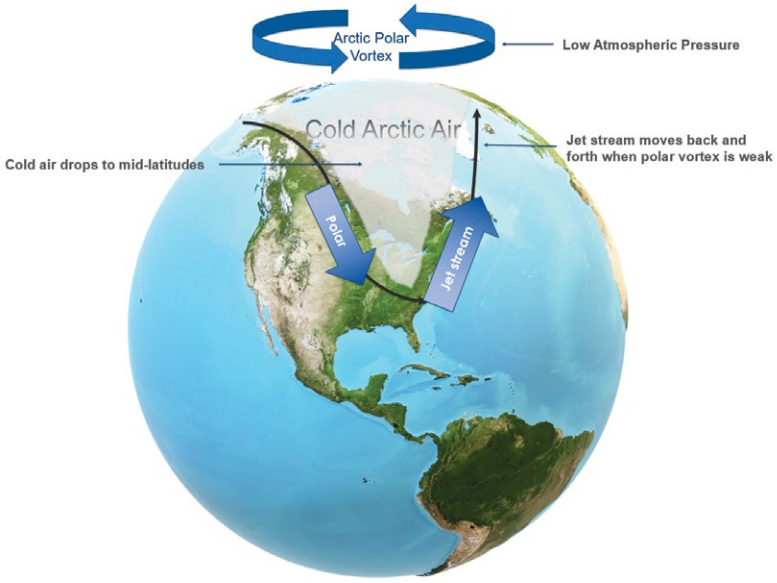
Examining polar vortex trends

In the past 40 years, the polar vortex has exhibited weakened states with greater frequency. The consequences of this trend have direct implications on day-to-day life in many densely populated regions, as well as at a macro level with respect to the changing climate.

When polar vortex disruptions transpire, severe winter weather, such as cold air outbreaks and heavy snowfalls, are more common for the subsequent four to six weeks or longer. Within the past four decades, we've observed more severe weather from this weakening. What's more, the increased frequency of vortex splits may be creating a feedback loop that accelerates even more splits in the future.

To best illustrate this feedback loop, let's begin in the summertime, when increasingly warmer temperatures in the Arctic are contributing to more extensive ice melt. In the summer of 2019, 12.5 billion tons of ice melted in Greenland in just one day, the highest recorded single-day loss since measurements began in 1950.[3] It also appears that the extent of Arctic sea ice observed in September 2019 was the second lowest on record.

How could this summer ice melt contribute to polar vortex disruptions in the winter, nearly half a year later? Ice functions a bit like an arctic mirror, reflecting sunlight and heat back into the atmosphere. Water, on the other hand, absorbs and retains heat. As a greater percentage of the ice in this territory melts and is replaced with water, heat that would typically be sent back into space is instead trapped in the water. In the fall, when



polar air masses turn cold, the heat contained by the water is released into the atmosphere (since heat flows from warm to cold) and modifies the hemispheric air flow, weakening the polar vortex. Such disruptions take some time to manifest into a polar vortex split, which is why the effects aren't felt until wintertime.

This feedback loop, labeled "Arctic Amplification" by some scientists, can continue after a split occurs. The warmer air that infiltrates the Arctic during a split in the winter limits the ability for ice to be built back up, thus perpetuating the cycle of absorbent water supplanting reflective ice. This cycle contributed to record-low sea ice around Alaska in the winter and spring of 2019, with great disruption to the local ecosystem.[4]

Are the polar vortex developments of the past few decades indicative of a significant long-term trend? At this point, we can't say for sure. However, if these splits do continue to emerge into a winter-time ritual, preparations for these crippling arctic events in the winter time may soon be imperative.

Contributors
Judah Cohen, PhD is Director, Seasonal Forecasting, Atmospheric and Environmental Research (AER).
Peter Sousounis, PhD is Vice President, Director of Climate Change Research, Research and Modeling Division, AIR Worldwide.

Sea Level Change: Examining Hot Spots and Their Potential Implications for Insurance and Society

By: Christopher Little

Increases in the frequency and severity of coastal flooding due to sea level rise are resulting in substantial impacts to coastal infrastructure, regional economies, the insurance industry, and society at large. Without additional flood protection measures, economic costs resulting from this peril are estimated to exceed US $1 trillion by 2050.[1] These costs will not be distributed evenly around the world, in part because sea level changes are not occurring at the same rate everywhere. This brief summary examines some of the factors underlying **hot spots**—areas where sea level is rising more rapidly than other locations.

How sea level rise affects coastal flooding

Sea level rise is often envisioned as the gradual inundation of coastal regions. While this is technically true, what we observe is more complicated: The long-term rate of sea level rise is obscured by the short-term variability of storm surges and tides. When the average (or mean) sea level rises, the maximum water level of every high tide and storm is a little higher. Over long periods of time, or when rapid (a period of several years) increases in mean sea level occur, flooding is more frequent, and any particular flood event is a little more severe. Thus, the rate of sea level rise (among other factors*) determines changes in the severity and frequency of coastal floods.

The rate of sea level rise varies widely at local (kilometers), regional (hundreds of kilometers), and ocean basin (thousands of kilometers) scales. This spatial variability is the combined effect of many physical processes, operating over seconds to millennia, that influence both the motion of the ocean and the land.

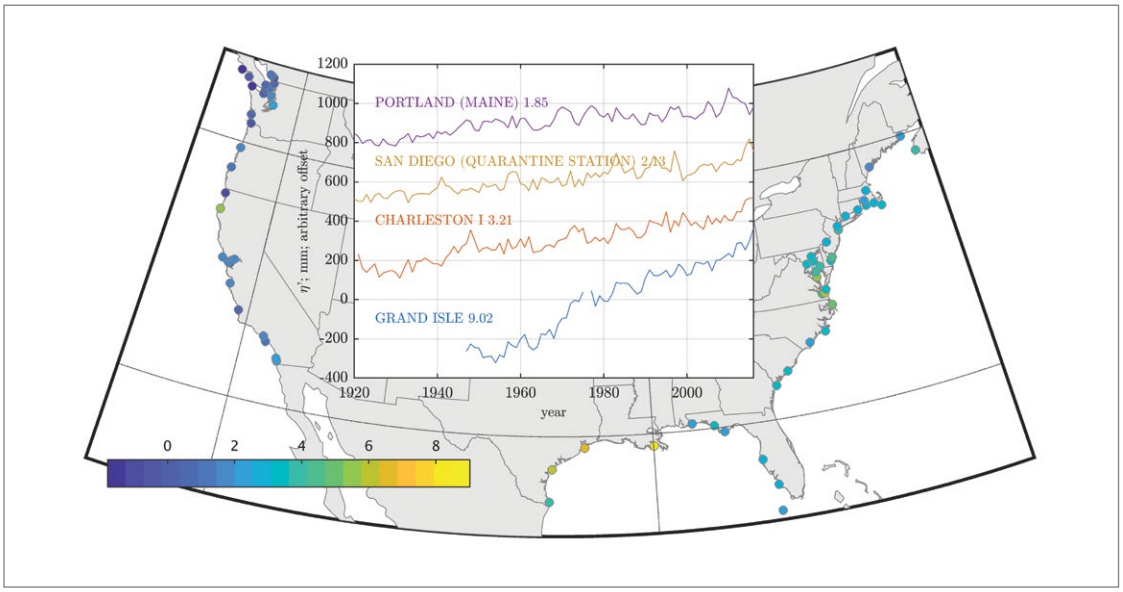
These processes include:

- ocean density and circulation changes
- addition of water from melting glaciers and ice sheets
- gravitational and rotational effects associated with melting ice that alter the height of the sea surface and the land
- the ongoing response of Earth's mantle to past changes in ice sheets (for example, the last ice age approximately 20,000 years ago)
- sediment compaction that can be accelerated by groundwater or hydrocarbon withdrawal
- earthquakes

* This summary focuses on the influence of changes in mean sea level on flooding. Climate change influences the frequency and intensity of storms, and human modifications (for example, harbor dredging or wetland development) affect storm surges. There are strong signs that these changes indicate regional hot spots. There are also places where flood frequency or severity will increase more for a given sea level rise due to the local flood regime or coastal defenses.

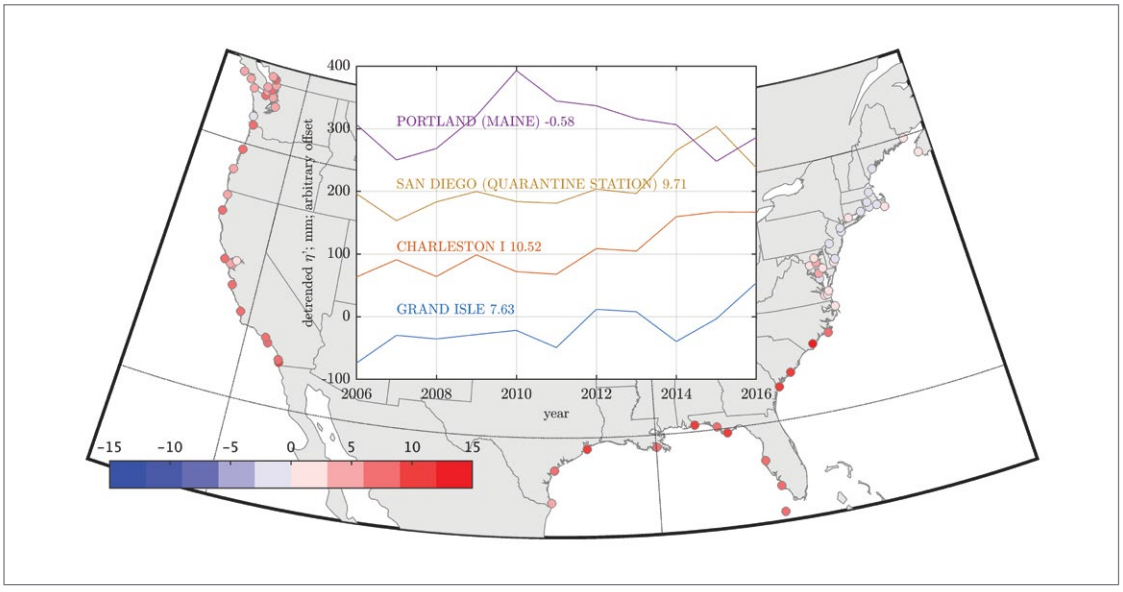
The importance and magnitude of each of these processes varies depending on geographic location, driving regional differences in the rate of sea level change along global coastlines. The figure below highlights observed variations in sea level trends in the United States. Other global locations also show high spatial variability in the rate of sea level change.

Figure 1



Colored circles correspond to trends in sea level at U.S. tide gauges with records longer than 30 years. Inset shows 1920–2016 tide gauge sea level at four tide gauges, with numbers indicating the long-term linear trend.

Figure 2



This is similar to the top panel but showing the difference between 2006–2016 trends and the trend over the record length (note larger scale). Inset shows 2006–2016 at four tide gauges, with numbers indicating the 2006–2016 linear trend. The data is from the Permanent Service for Mean Sea Level (PSMSL), retrieved December 19, 2018. All values in mm/year.

Sea level trends: A few examples of hot spots

The most prominent U.S. sea level rise hot spot is along the Gulf Coast. Parts of Louisiana are experiencing a long-term rate of sea level rise of almost 1 centimeter per year. This rate is nearly ten times higher than the global mean sea level rise rate of 1.2 mm/year between 1900 and 1990, and approximately three times the global mean rate since 1990. This hot spot is largely the result of land subsidence (sinking) due to the extraction of oil and other hydrocarbons. Subsidence is even more dramatic in Southeast Asia, such as in Jakarta and Tokyo, where parts of both cities have sunk by several meters. Much of this subsidence is due to groundwater extraction and compaction from urbanization and development. Sea level rise thus interacts with local water stress, another significant climate risk.

In the United States, sea level is generally rising faster along the East Coast than the West Coast. This is largely related to the long-term effects of previous ice ages, especially in the mid-Atlantic. Additionally, there's likely some long-term enhancement of east coast sea level rise due to weakening of the North Atlantic Ocean circulation, including the Gulf Stream. In regions close to glaciers and former ice sheets, sea levels fall as the land rebounds from the ice load. For example, the sea level in Juneau, Alaska, is declining by more than a centimeter per year as nearby glaciers melt. While falling sea levels decrease coastal flood risk, they may interfere with coastal infrastructure and port operations.

> "Without additional flood protection measures, economic costs resulting from this peril are estimated to exceed US $1 trillion by 2050."

The location of hot spots differs depending on the time frame considered. For example, over the past ten years, rates of change have varied widely regionally due to atmospheric and ocean variability and have often been much larger than long-term trends (lower panel). For example, over the past decade, the southeastern U.S. coast has experienced sea level rise rates up to three times higher than the global mean. Along the southeastern coast, this is manifesting in recurrent nuisance or sunny-day flooding. The U.S. West Coast has also experienced high rates of sea level rise, following a 20-year period of suppression. On the U.S. east coast, the dramatic 2008–2010 sea level rise event dominates the variability in the Portland, Maine, record over the last decade. This three-year event was equivalent to 30-plus years of global mean sea level rise, sufficient to have substantial implications for coastal flooding. Short-term decreases are also possible. For example, Portland's sea level decreased following the 2008–2010 rise.

Outlook

Some of the drivers of regional hot spots are likely to persist into the future: For example, the rate of subsidence caused by geological factors is not expected to change for thousands of years. On the other hand, human-caused subsidence can be slowed by reducing extraction of subsurface fluids; this has been accomplished successfully in Tokyo. Hot spots due to ocean variability should be expected to change over time due to both natural and human-driven changes in the ocean. Over the second half of this century, the regional rate of sea level rise will largely be caused by the input of water from melting glaciers and ice sheets. The rate of melting is, at least partially, in our control through climate policy.

Even with strong, concerted action to reduce carbon emissions, it's likely that many coastal residents and businesses will confront an acceleration in sea level for the foreseeable future. A recent paper[2] highlights four general approaches to coastal adaptation:

1. accommodation of more frequent flooding through social (improved emergency response), economic (flood insurance), and engineering (building elevation) changes
2. creating or augmenting man-made and natural defenses against flooding
3. reclaiming land from the ocean
4. relocation through planned or unplanned migration

Determining the optimal combination of these approaches requires consideration of the current and future physical setting as well as decision-making strategies that account for uncertainty and political and sociological barriers.

The insurance industry can help reduce losses by anticipating increasing losses to public and private sectors from nuisance flooding. Additionally, risk modelers should integrate the improving scientific understanding of the physical processes that modulate observed and expected changes in regional flood risk. Efforts to incorporate the time-varying and spatially differing drivers of flood risk into catastrophe models are particularly important.

Contributor

Christopher Little is Senior Staff Scientist, Atmospheric and Environmental Research (AER).

Where Climate Change and Natech Risk Meet

By: Alastair Clarke

Insurers want to know when and where a climate change signal will appear in their loss record. Sea level rise **(read more on pg. 10)** is one of the clearest signals of Earth's response to global warming. And given that changes in mean sea level (MSL) will drive changes in future extreme sea levels, monitoring coastal properties to spot the emerging climate change trend is paramount. This article considers the large industrial facilities along the Gulf Coast. These sites are exposed to physical, transition and liability risk. Casualty claims can be triggered by natural disasters, and as sea levels rise, more severe claims could emerge.

> "Between 1990 and 2008, natural hazards were the cause of 16,600 reported hazardous releases. . ."

Accidents in the industrial sector can be catastrophic, and up to 5 percent of all accidents in this sector are caused by natural events.[1] Between 1990 and 2008, natural hazards were the cause of 16,600 reported hazardous releases and more than 70 percent were due to climate perils such as hurricanes and precipitation.[2] In each case, a natural event triggered a technological malfunction that led to the release of hazardous material (hazmat). This kind of event is called a **natech**, short for natural-technologic. The insurance implications for these events are significant.

Casualty liability from natural disasters

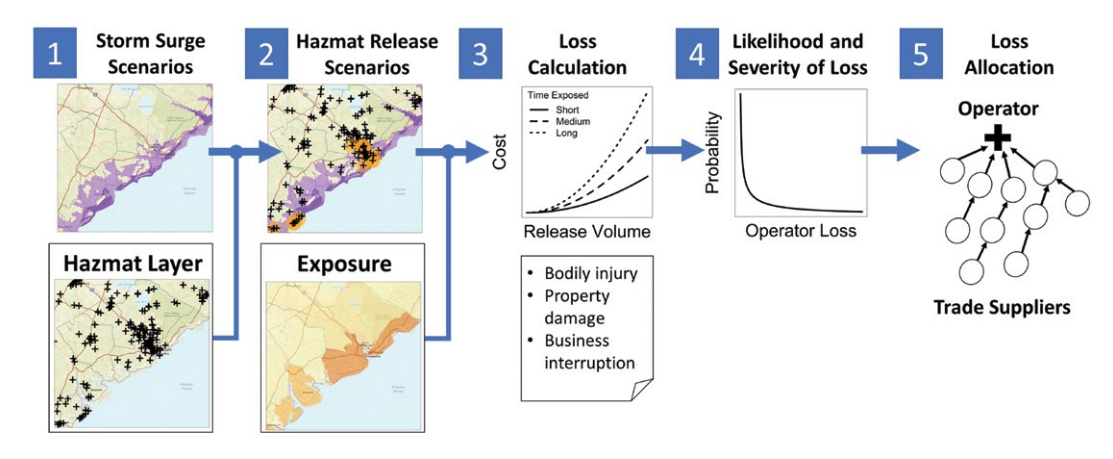
There are many examples of catastrophic casualty claims from natechs. In 2010, a wet summer contributed to the collapse of a dam at the Ajka alumina plant in western Hungary. The resulting toxic sludge spill caused ten deaths, 150 injuries, and environmental contamination. The plant was fined GB £330 million.[3] In 2005, Hurricane Katrina triggered 200 hazmat releases. The costliest occurred when storm surge waters ruptured a storage tank at the Murphy Oil refinery in Louisiana. The release of 25,000 barrels of crude oil affected 1,800 homes and resulted in a US $330 million settlement.[4]

The operators of industrial facilities and other hazmat sites perform hazard analyses to anticipate such events and consider whether their existing safety mechanisms are adequate. If a hurricane triggers a hazmat release, the operator of the offending site can be found guilty of negligence if reasonable measures were not taken to prevent the release, even though the ultimate cause of the disaster was a so-called *natural* event.

Natech catastrophe models

A catastrophe model (cat model) is designed to calculate the likelihood and severity of financial loss from extreme events. Since the 1980s, these models have been used by insurers to prepare for earthquakes and hurricanes, and more recently they have been built for man-made perils such as terrorism and cyber incidents. A framework for a natech cat model that estimates casualty loss from storm surge is presented in **Figure 1**.

Figure 1. Natech catastrophe model framework for quantifying liability from storm surge.



There are five stages in this framework: In **stage one**, thousands of storm surge scenarios are simulated from a physics-based, stochastic model such as AIR's Hurricane Model for the United States. Each scenario footprint is intersected with a hazmat layer (a map of industrial facilities and superfund sites that contain hazardous materials).

Each surge scenario can trigger a variety of hazmat release scenarios. In **stage two**, the surge scenario has triggered a toxic plume from a chemical plant and an oil spill from a refinery. The orange circles represent contamination zones that intersect with the people, residencies, land, and commercial buildings found in exposure maps.

In **stage three**, the costs of each hazmat release scenario are calculated using statistical models that relate hazardous release and exposure time to loss. Historical claims from bodily injury, property damage, environmental clean-up, and business interruption can be used to build such models.

In **stage four**, losses from all scenarios are tallied to give a probability distribution of expected loss. The losses are calculated for the insurer who indemnifies the operator of the hazmat sites.

The culpability for the loss may not lie with the operator but could instead lie with the operator's suppliers who did not correctly install the control valves at the chemical plant or the flood defense at the refinery. In **stage five**, a liability footprint shows which suppliers might be liable with the arrows representing flow of trade to the operator. Arium's software considers this footprint as well as other mechanisms to allocate the loss.

This conceptual framework helps identify the datasets and tools needed to build a natech cat model. It also reveals how liability risk is sensitive to climate change as well as other *acts of man*.

Natechs and climate change risk

Natech risk, measured as the number of natech events per number of hazmat sites, has historically been highest in the Gulf Coast states.[5] This region is the center of the U.S. petrochemical industry and is exposed to significant hurricane risk. Hurricanes from the Atlantic can approach the Gulf Coast bringing extreme winds that cause severe structural damage and storm surge that leads to extreme sea levels and flooding. Compounding this issue, the Gulf Coast has experienced prominent MSL rise along the coast due to land subsidence from groundwater extraction, and its MSL will continue to rise due to the thermal expansion of the oceans and the melting of ice sheets.

Cat models are usually designed to quantify the present risk posed by a peril, but they can also show the financial implications of future climate projections. In 2010, AIR used the U.S. hurricane model to show that the physical risk from storm surge along the Gulf, measured as the average annual loss per dollar of exposure, would increase by as much as 20 percent by 2030.[6] The Mississippi Delta, the Gulf Coast of Florida south of Tampa Bay, and Cape Hatteras were identified as regions most at risk from a higher MSL and a warmer Atlantic.

Because storm surge can trigger natechs, liability risk in the Gulf should increase too. However, it must be recognized that the number of hazmat sites will change over time and could decrease if our society transitions from a petroleum-rich economy to a low-carbon one. This suggests the petrochemical industry in the Gulf has significant transition risk **(read more on pg. 17)** in addition to physical and liability risk.

Cui culpa?

Natechs show how liability can arise from natural events that can be traced back to the suppliers of a faulty service. With land subsidence from groundwater extraction, the culpability could be traced back in a similar way. However, with climate change, the threads are deeply tangled. It's difficult to prove that climate change caused a specific storm surge event. We can only argue probabilistically and say climate change has made events like this more likely to occur. However, there are numerous cases, albeit none yet successful, against major oil producers that attempt to hold them liable for their contribution to climate change.

Natural disasters were once known as acts of god, while man-made was reserved for perils of human agency, like terrorism. As we become more aware of what exacerbates catastrophe risk and we place higher expectations on companies to take preventive action, the blame could shift from deity to company.

Contributor
Alastair Clarke is Research Associate, AIR Worldwide.

Climate Change: Transition Risks

By: Olivia Dobson, Richard Hewston, and Will Nichols

The tangible nature of the physical impacts of climate change means that other aspects of climate risk can often be overlooked. **Transition risks**—the challenges posed by actions to lessen greenhouse gas (GHG) emissions in our societies—are an example of this and can be just as relevant and impactful for businesses around the world as physical risks. As both investors and providers of risk-transfer devices, the insurance industry is exposed to the consequences of transition actions as well as the more palpable threats presented by the changing climate.

Following the Paris Agreement, which became effective in November 2016, governments across the globe are in the process of imposing more stringent GHG emissions regulations to mitigate the effects of climate change. Identifying and managing the transition risks associated with these regulations is vitally important to companies across all sectors as the world moves toward a low-carbon economy.

For businesses, transition risks can manifest in several ways:

- **Stranded assets:** In economies transitioning to lower-carbon emissions, stranded assets refer to those assets and investments that are reduced in value as a result of their association with carbon-intensive activities.

  The future production and use of approximately US $2.3 trillion of upstream oil and gas assets is inconsistent with global commitments to limit worldwide temperature increases to 2˚C. To deliver the pledges made under the Paris Agreement, business as usual is not a viable option for fossil fuel companies or their investors.

  But other sectors are also at risk: CDP (formerly the Carbon Disclosure Project), a nonprofit independent reporting organization, has found that almost US $950 billion of publicly listed companies' turnover will be threatened if governments move to halt activities driving deforestation (a source of emissions). Additionally, investors have concerns regarding the carbon-intensity of shipping and transportation activities, as well as potential lost revenues in the sector if carbon policies restrict the production and movement of coal, oil and gas, and other commodities.

- **Disclosure:** Companies across all sectors, but especially financial institutions, are increasingly expected to apply the Recommendations of the Task Force on Climate-related Financial Disclosures (TCFD) to assess and publicly report on their exposure to climate change for both physical and transition risks. Aside from the complexities of predicting these impacts, public disclosure may reveal risk exposure and internal management strategies that affect the value and/or reputation of a company, such as by negatively impacting an enterprise's ability to raise capital.

- **Litigation:** Potential liabilities exist for companies directly or indirectly associated with large amounts of GHG emissions. Several lawsuits have been brought against multinational corporations (oil and gas companies in particular) attempting to place responsibility for future climate change–related impacts

with these enterprises. The number of climate litigation cases has grown sharply since 2004, with most occurring in the United States. From 2004 to 2018, almost 1,000 cases were filed in the U.S., while fewer than 270 suits have been filed in all other countries combined.

Perhaps the most eye-catching lawsuit was brought by New York City in 2018 and sought billions from the five largest publicly traded oil majors to compensate for the city's investment in climate resilience measures. It was later dismissed, and although a large proportion of the other cases will also be unsuccessful, all it takes is one successful case to set a precedent that triggers a flurry of lawsuits. Companies should be aware that courts have the power to issue substantial financial penalties. As the impacts of climate change become more apparent, there's a real possibility that courts may wield this power more aggressively.

- **Reputational threat:** Many businesses are coming under pressure to distance themselves from fossil fuel–dependent industries, activities, or projects, both through the withdrawal of services and via divestment. Association with emissions-intensive undertakings can make a business the target of damaging protests and negative campaigns.

- **Operational costs:** A significant portion of the near-term investment costs that are required to rebalance an economy toward becoming more energy-efficient and less carbon-intensive is likely to be passed on to business: For example, through higher energy prices or more stringent energy-efficiency standards. Alongside this, businesses in carbon-intensive markets may be faced with new legislation, such as emissions trading schemes, that prompt unexpected capital outlays.

The insurance sector faces further unique challenges around transition risks. These include anticipating the consequences of policy and regulatory changes for their clients and adapting products and coverage to react to new and emerging circumstances and technologies.

Using data to understand transition risk exposure

While decarbonizing the global economy is undoubtedly a positive move for the planet, the associated risks for business can be difficult to quantify. For instance, how can investors identify geographies where regulation intended to limit carbon emissions is more likely to occur? This type of information can help investors determine how their portfolios could be affected.

Case Study

Verisk Maplecroft's Carbon Policy Index has been devised to help companies identify where policy changes driving transition risks pose the greatest threat. It assesses the potential for more stringent GHG emissions-reduction policies to be implemented across 195 countries and the degree to which those policies are likely to have material implications for business. The index is scored on a 0–10 scale, where 0 indicates the greatest risk.

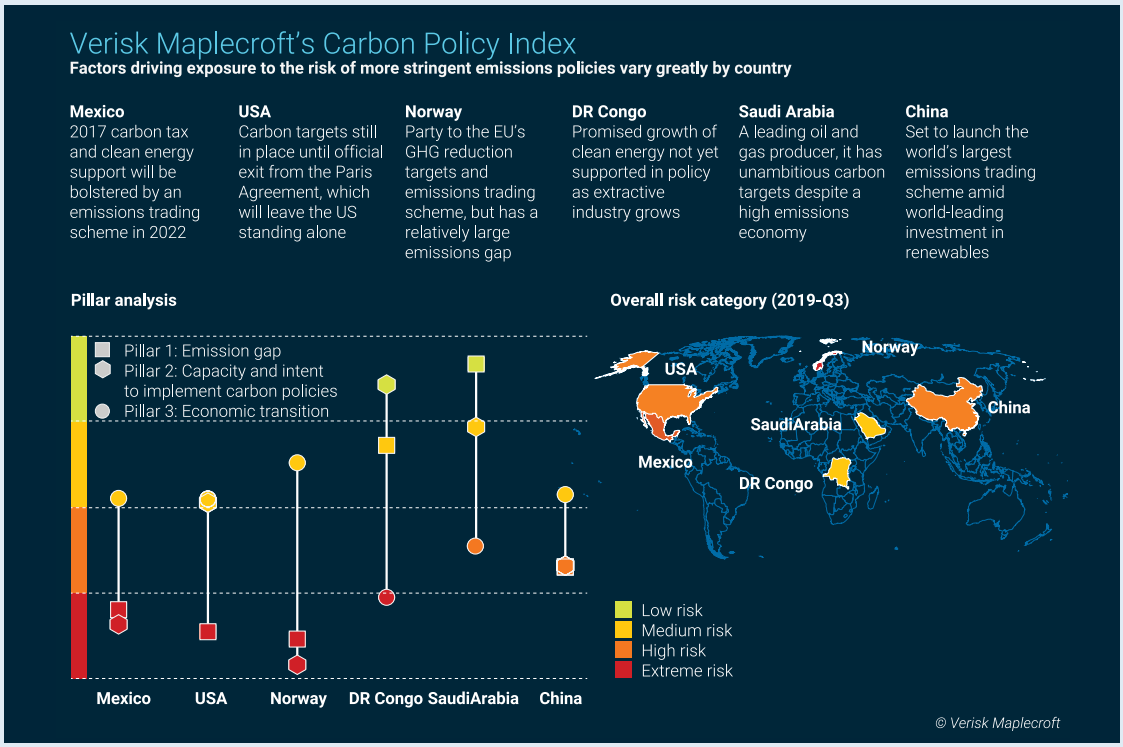
The index uses three pillars to examine the level of risk present. It considers:

1. the extent of the gap between a country's current emissions levels and its stated targets
2. the capacity and political will to implement carbon reduction policies successfully
3. the trend in the recent carbon intensity and energy efficiency of its economy

Countries with larger emissions gaps will require more stringent mitigation measures to meet targets, while new or more stringent carbon policies are likely to have greater financial implications for companies

operating in markets that are highly energy-intensive, are heavily reliant on fossil fuels, and show little recent progress in improving these factors.

The majority of the highest-risk countries in the index are located in Europe, with Iceland (ranked 1st), Finland (2nd), Portugal (3rd), Norway (4th), Austria (5th), Switzerland (8th), and France (9th) making up seven of the nine countries categorized as “extreme risk.” New Zealand (6th) and South Korea (7th) complete this group, all of which feature significant emissions gaps in achieving their stated targets alongside considerable levels of capacity and intent to implement policies to meet these commitments.



Topping the index is Iceland, whose economy is also relatively energy-inefficient compared with the other extreme risk countries.

The data within the index pillars identifies the key drivers of risk, providing insight into the nature of the challenges present in each individual geography. The visual above illustrates the risks present for a selection of countries.

As pressure increases from regulators, corporate boards, and shareholders to understand the financial, operational, and reputational implications of the move toward a lower-carbon economy, developing an in-depth understanding of the range of ways in which transition risks could affect business activities is a growing challenge for risk managers in all sectors.

Contributors

Olivia Dobson is Principal Analyst, Risk Analytics, Verisk Maplecroft.
Will Nichols is Head of Environment and Climate Change Research, Verisk Maplecroft.
Richard Hewston is Principal Consultant, Environment, Verisk Maplecroft.

Cyber Security

22 Power Utilities Face Emerging Cyber Threats

25 Cyber Risks Loom Large in an Interconnected World

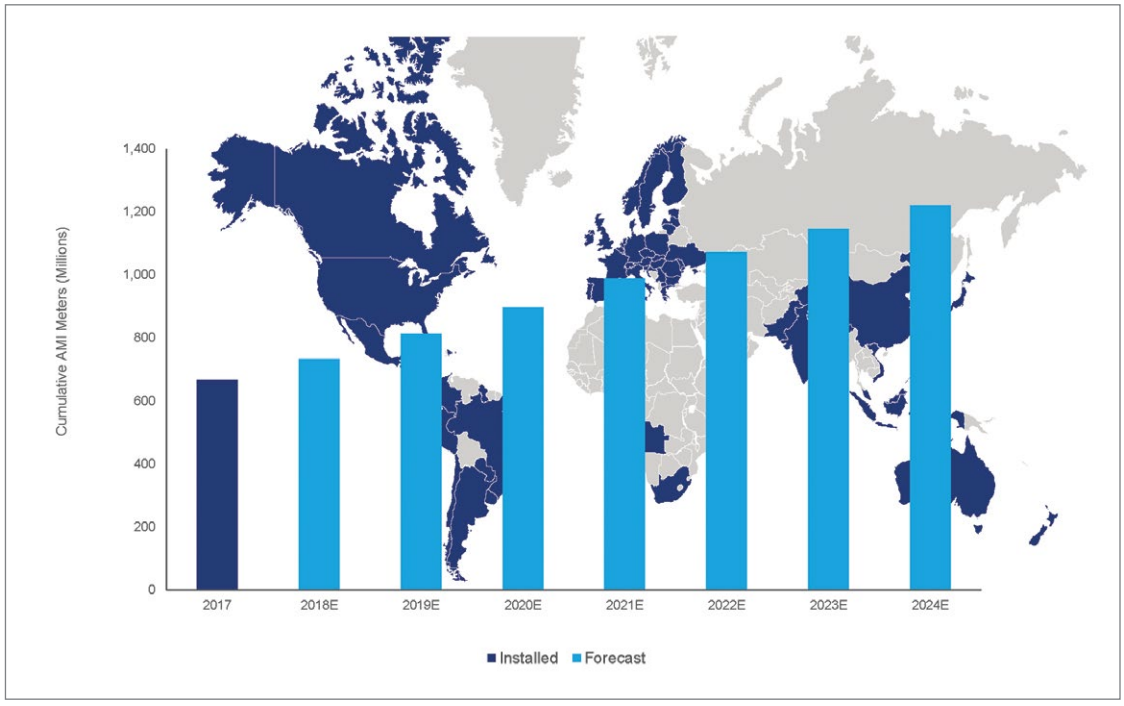
28 Could NotPetya's Tail Be Growing?

30 Cybersecurity Needs a Quantum Leap

Power Utilities Face Emerging Cyber Threats

By: Ben Kellison

Security threats in the power industry continue to proliferate as utilities become more digital and customer-centric. Utilities are focusing security efforts on traditional operational threats, such as cyber intrusions, as well as risks that could correspond with the burgeoning world of Internet of Things (IoT) devices. As more IoT devices interact with the grid and with power utilities, they create millions of new pathways that must be safeguarded from cyberattacks. Finally, the dangerous threat of physical attacks on power infrastructure continues to loom.



Smart meters are the most common utility connected device around the globe. There will be more than 1.2 billion units installed and communicating by 2024, with Asia driving global growth. Our forecast covers 80 countries, across six continents, accounting for more than 5.3 billion people.

SCADA's role in power grid vulnerabilities

Utilities were early adopters of Supervisory Control and Data Acquisition (SCADA)-based solutions to help access data and control far-flung assets on the grid. SCADA, a type of industrial control system (ICS), was developed before the Internet became ubiquitous; thus, it was designed to be simple and operate in a closed system without any connections to the outside world.[1]

However, in the last decade, the number of devices added to these control networks has exploded as utilities continue to seek more visibility into the power distribution grid. These devices introduce new security vulnerabilities to SCADA-based systems and the grid they control. Moving forward, cybersecurity for the full-range of power generation, transmission, and distribution assets will likely involve different approaches, very often requiring different levels of oversight.

> "Utilities alone are expected to deploy more than 800 million connected IoT devices by the end of 2019. Each of these are potential gateways for cyberattacks…"

The rising frequency and severity of cyberattacks on energy and utility infrastructure have only served to heighten this need.

Traditional operations threats

In December 2015, several Ukrainian distribution utilities' networks were compromised in a multi-month attack. The breach began with spear phishing and malware tactics to gain access to corporate networks, then escalated with the remote seizure of the utilities' network control systems, systematic switching off of key substations, and the disabling and destruction of both key field control assets and company files.[2]

This coordinated and advanced attack was attributed to state actors and led to a renewed focus and concern about the technical savvy of potential attackers.[3]

IoT entry threats

New cyber threats for utilities are emerging, including from:

- the digitization of distributed assets, such as smart meters, new sensors, and power electronics equipment
- tremendous demand to invest in new customer and utility energy generation
- loads and monitoring devices at the edge of the grid

Utilities alone are expected to deploy more than 800 million connected IoT devices by the end of 2019.[4] Each of these are potential gateways for cyberattacks into one or more of a utility's systems. The grid is also becoming more decentralized. Tens of millions of small generators and loads are being integrated into more power markets and local power systems that may or may not be owned or operated by the utility.

As more of these resources participate in power markets and utility programs, power systems are expected to become more reliant on these resources, as well as the dozens of corporate clouds that are aggregating and dispatching resources both for customer benefit and power market participation.

This will likely increase the grid's exposure to cyber events that may affect appliance manufacturers, HVAC and HVAC control suppliers, and e-mobility firms. These firms' products will increasingly compete with traditional and renewable power plants not just to address peak load challenges but also to provide grid services that maintain the balance of supply and demand.

The trend may persist in the future as many utilities and aggregators are expected to continue to embrace advances in communications and control technologies, leading to new cyber challenges.

Physical security threats

While cybersecurity is a hot topic, there's also renewed concern about physical risks, in part due to the 2013 attack on PG&E's Metcalf substation. This attack featured a small team cutting some of the fiber communications lines to the station while enlisting a sniper to shoot at 17 electrical transformers. The coordinated effort ultimately led to more than US $15 million in damages inflicted in just 20 minutes.[5] Following the attack, a member of the FBI suggested that the operation didn't require "a very high degree of training" to execute.[6]

Fears of physical strikes on critical infrastructure were heightened in the wake of the 2019 drone or missile attacks on 17 structures in the Khurais oil field and Abqaiq refining facility in Saudi Arabia's Eastern Province.[7] The strikes disrupted the production of 5.7 million barrels of oil per day, leading to a spike in crude oil prices around the globe.[8] These strikes demonstrate both the velocity and potentially global impact of physical strikes on energy resources. The proliferation and continued advancement of drones and other smaller precision weaponry are an emerging threat to critical infrastructure in areas with simmering geopolitical tensions.

Contributor
Ben Kellison is Director, Power & Renewables, Wood Mackenzie.

Cyber Risks Loom Large in an Interconnected World

By: Tim Campbell and Kamban Parasuraman

In recent years, corporations have been exposed to more supply chain risks than ever before. Various factors, including geopolitical disputes and climate change, can contribute to changing supply chain exposure footprints. However, increased vulnerability to malicious cyber activity in particular has emerged as a key concern for many companies. A recent survey of more than 1,000 UK and U.S. chief information security officers and other risk professionals indicated that the average company shares confidential information with about 583 third parties.[1] This exchange of data and sensitive information increases the risk of data breaches; 59 percent of the companies surveyed experienced a data breach linked to one of their vendors or separate third parties in 2018.[2]

Additional data from the National Institute of Standards and Technology (NIST) also casts a light on cyber risks caused by vulnerabilities in the supply chain. According to NIST, nearly 24 percent of supply chain disruptions are caused by cyberattacks.[3] Supply chains also represent a primary target for hackers, with 80 percent of information breaches originating in the supply chain.[4]

A couple of widely reported examples of major cyber incidents inflicted through vendors of large enterprises include:

- **Facebook:** A Mexican social media firm's (Cultura Colectiva) unprotected Amazon cloud computing service exposed more than 540 million Facebook users' account names, ID numbers, comments, and reactions.[5]
- **Target:** In 2013, the credentials of a third-party vendor were used to breach 70 million customer records.[6] The attackers reportedly stole the credentials of a heating, ventilation, air conditioning (HVAC) subcontractor that had been accessing Target's network through an external vendor portal.[7] In total, the breach cost Target nearly US $300 million in legal settlements.[8]

Contingent business interruption: A key cyber exposure in the supply chain

Contingent business interruption (CBI) is the disruption to a company's operations resulting from the interruption of a service provided by a vendor in the company's supply chain. A cyberattack can affect common third-party vendors, such as cloud service providers, Internet service providers, payment processors, domain name system providers, e-mail servers, content delivery networks, and ad networks. A security or system failure of any one of these services can result in a major outage and financial loss to another company. The threat of CBI is growing rapidly as organizations migrate to the cloud, where an outage could affect numerous organizations across the industry. Similarly, increased interconnectedness of industrial automation and control systems (IACS) and Internet-connected IT networks have added a new layer of threat for cyber-triggered supply chain disruptions. For example, in March 2019, Norsk Hydro, one of the world's largest producers of aluminum, was forced to run some operations manually because of a cyberattack to an Internet-connected IT network.[9]

To mitigate exposure to CBI risks that emanate from cyberattacks, corporations should continuously identify and monitor their third party interdependencies.

When sizing up third-party relationships for potential cyber risks, companies should consider:

- Which partners do these enterprises engage with?
- What services and products are provided by a third party?
- What type of data is being exchanged?
- What kind of network access is being granted?

How can insurers manage an interconnected book of business?

Just as companies need to be aware of the cyber risks introduced by third parties in their supply chains, insurers may need to consider how the insureds within its own book of business are interconnected. In fact, the lack of full visibility into each insured's interdependencies may create risks that are unidentifiable from an underwriting standpoint.

To account for the uncertainty arising from data and knowledge gaps, some insurers may resort to a qualitative, faith-based, piecemeal approach for CBI underwriting. However, without considering the correlation across suppliers and service providers, products, and industries, this fragmentary approach to CBI risk underwriting can result in risk aggregation creeping into an insurer's portfolio, where a large-scale event can lead to catastrophic accumulations. To be resilient against these new vulnerabilities and threat vectors, it is important for the insurance industry to take a holistic view when assessing the interconnected risks.

Using technology and analytics to measure supply chain risks

Across organizations, the Industrial Internet of Things (IIoT) is enabling many companies to track, measure, and optimize elements of their supply chain. For example, IIoT is set to replace barcodes and scanners with radio-frequency identification (RFID) technology, cloud-based GPS sensors, and in-vehicle monitoring technologies that will enable companies to track and monitor the location and condition of products from source to end-delivery point.[10] For this emerging risk, the insurance industry cannot rely solely on old techniques of taking historical claims data and projecting it forward.

Machine learning, and other promising predictive methods, can be deployed to identify trends and intangible aggregation scenarios from diverse supply chain data, including information provided by the IIoT, allowing us to continually improve our understanding of interconnected risks. The rich set of analytics and insights gained from these predictive methods enable risk managers and insurers to transition from reactive to proactive management of their supply chain risks. They can identify interdependencies before events happen, allowing companies to future-proof their businesses against probable impending contingencies.

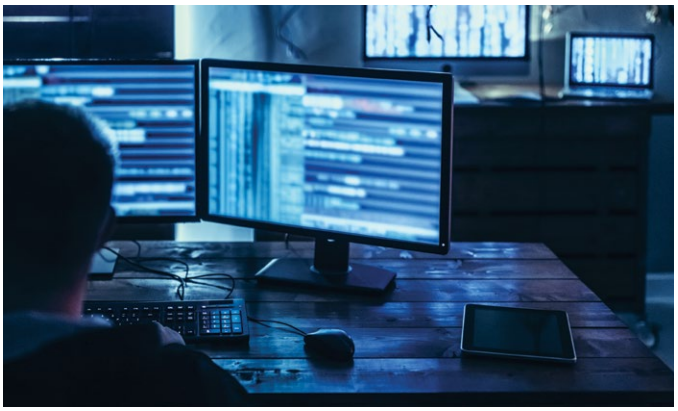
AIR Worldwide has experience modelling similar emerging risk scenarios. For additional information, please see Lloyd's innovation report **"Hidden Vulnerabilities in Supply Chain Risk: A Quantitative Risk Modelling Framework" at** https://www.lloyds.com/news-and-risk-insight/risk-reports/library/understanding-risk/hidden-vulnerabilities

Contributors
Kamban Parasuraman is Principal Engineer, Manager, AIR Worldwide.
Tim Campbell is Senior Analyst, Country Risk Analytics, Verisk Maplecroft.

Could NotPetya's Tail Be Growing?

By: Tom Johansmeyer

Cyber catastrophe risk has been difficult to understand and analyze. For example, it initially looked like the cyberattack dubbed NotPetya would be a somewhat benign cyber catastrophe, leading the market to question the prevailing wisdom about the long-tail risks from professional lines (such as directors and officers, or D&O). However, the event evolved, offering a learning opportunity from the first PCS®-designated global cyber catastrophe.



Lesson 1: It's tough to predict exploding cyber cats

Careful analysis would normally be the solution to understand cyber catastrophes, but there's minimal information available to conduct this sort of effort. The PCS team looked at the economic losses from major cyber events over the past 20 years, with a dozen of them reaching at least US $500 million. While every major event comes with lessons for risk bearers, fast-changing circumstances compounded by time can erode the benefits of learning from the past and hamper capital deployment.

Historical Cyber Events: Economic Losses

Event	Year	Economic Impact
Melissa	1999	US $1.2 billion
ILOVEYOU	2000	US $15 billion
Code Red	2001	US $2 billion
Sircam	2001	US $1 billion
Nimda	2001	US $635 million
Sobig	2003	US $37 billion
SQL Slammer	2003	US $750 million
Mydoom	2004	US $38 billion
Sasser	2004	US $500 million
Conficker	2007	US $9.1 billion
WannaCry	2017	US $4 billion
NotPetya	2017	US $10 billion

Source: PCS internal research

Only two of the above cyber catastrophes resulted in directly meaningful losses for the global insurance industry: WannaCry and NotPetya. WannaCry caused significant economic losses, but the impact on the insurance industry amounted to only US $50–60 million. NotPetya, by contrast, had insured losses of above US $3 billion—and the event is still developing. Another, LockerGoga, seemed poised to cause nontrivial insured losses industrywide. Following the Norsk Hydro affirmative cyber loss, though, it looked like momentum slowed a bit, with the five other companies being monitored appearing to have economic exposure but little in the way of insurance implication. (PCS continues to monitor LockerGoga for insurance industry developments.)

Lesson 2: It's about much more than the cat's tail

So, what makes WannaCry and NotPetya different from each other? Some believe that WannaCry's economic impact was actually greater than that of NotPetya's, despite the imbalance in insurance industry implications.

NotPetya appears to have affected larger companies in a way that resulted in greater engagement with the insurance industry, given the business interruption implications that were relevant to property programs. That wasn't the only reason for the much larger loss reported for NotPetya. Two major risk losses contributed more than 80 percent of the event's insured loss of above US $3 billion. Without them, the overall insured loss—not to mention the economic loss—would have been much more modest, with the impact on the global insurance industry commensurate with that of a particularly nasty single-state hailstorm.

The dearth of precedent has caused the global insurance and reinsurance industry to examine NotPetya with particular care, combing it for every possible insight that could be used for analysis and prediction. Before this event, the global reinsurance industry was fixated on the effect that a cyberattack could have on the professional lines market, but the property losses from NotPetya shifted our community's focus. However, it's worth revisiting the potential concerns initially associated with professional lines claims from a cyber event. Based on developments in 2019, it appears that this issue is about to become relevant to the market.

In past years, there were concerns that a D&O claim represented the nightmare scenario for cyberattacks. D&O claims can drag on for years, and even successful claims handling can be an expensive and burdensome proposition.

> "WannaCry…amounted to only US$50–60 million. NotPetya, by contrast, had insured losses of above US $3 billion—and the event is still developing."

Perhaps to the relief of many, for the first two years of its development, NotPetya remained mostly a property event. Approximately 85 percent of the insured loss from the event was non-affirmative property. Although there had been some questions and concerns along the way, NotPetya became fairly stable faster than anyone expected for a cyber catastrophe. That's not to say the industry loss was approaching finality; there are always disputes in catastrophe events. But the process was fairly smooth.

However, a shareholder class action lawsuit filed nearly two years after the attack has introduced an added dimension for analysis involving the same D&O concerns that were initially feared, bringing a new source of non-affirmative insurance risks into the picture.

Contributor
Tom Johansmeyer is Head of PCS.

Cybersecurity Needs a Quantum Leap

By: David Geller

Perhaps no other technology on the horizon has simultaneously raised more hopes—and fears—than quantum computing.

While there are many differences between classical computers used today and quantum computers, the core of their capabilities differs with respect to bits and qubits.

Classical computers store and process information in bits, and each bit can exist in only one of two states (the classic 1 and 0 of binary code). But in a quantum computer, binary bits are replaced with qubits, which are units of computing information that exist in multiple states at the same time, thus allowing them to perform numerous calculations at once. Theoretically, this difference enables quantum computers to store and process much more information than their classical counterparts.[1]

If incorporated into encryption defenses, cybersecurity that features quantum computation could prove to be unhackable.[2] Conversely, if wielded by cyber criminals, quantum computers could trigger breaches at a truly unprecedented scale. Cyber paradise or cyber chaos looms.

Quantum computing's potentially colossal impact on the cyber universe is linked to how cybersecurity, namely encryption algorithms, operates. Contemporary data encryption is typically based on a complex series of math equations that classical computers aren't capable of solving, partially due to a lack of processing power.[3]

However, a quantum computer would theoretically possess much more processing power than classical computers and could harness that ability to solve the algorithm that's encrypting data. A sentiment among some researchers is that encryption methods tailored to classical computers would not be able to defend against a quantum-based attack. For example, a recent study indicated that RSA-2048, an encryption algorithm that computer scientists believe is impossible to breach by a classical computer, could be solved by a quantum computer with 20 million qubits in less than eight hours.[4]

Of course, this threat is unlikely to materialize until the distant future because a state-of-the-art quantum computer, as of 2019, has only 70 qubits.[5] Nevertheless, researchers and other experts have projected a timeline of roughly 10 to 20 years before hackers will have quantum computing at their disposal.[6]

Quantum-safe standards on their way

In 2012, the National Institute of Standards and Technology (NIST) began preparing for a world with quantum computers when they launched the Post-Quantum Cryptography (PQC) Standardization project. This effort attempts to ensure that computers are appropriately encrypted when quantum computers fall into the hands of bad actors.[7]

In 2017, NIST received 69 submissions for post-quantum cryptography strategies. In 2019, the agency trimmed down the list to 26 viable candidates. The efficacy of these algorithms will be tested broadly to determine if they are truly quantum-resistant. The expectation is that new post-quantum standards will be available before 2024,[8] and NIST has not ruled out that multiple algorithms could emerge as a viable standard.[9]

NIST isn't the only regulatory body that has attempted to foster development in quantum technology for cybersecurity purposes. The National Quantum Initiative Act was signed into law in 2018 and will allocate US $1.2 billion in funding to innovate and enhance quantum technology in the United States. Additionally, the Quantum Economic Development Consortium (QED-C), established by NIST, intends to cut the process of setting up a quantum research facility from three years to six months.[10]

Challenges with cybersecurity have set off a plethora of issues in the past ten years. Ultimately, the next decade may be defined by how quickly quantum computers—the true wild card of the computing universe—develops.

Potential risks from quantum computing

The immense processing capability of quantum computers could open up many possibilities—and potential risks. Here are a couple of potential exposures that loom in a quantum-computing era.

Long-tail consequences: Quantum computing might be the hacking tool of the future, but the data of the past could be most vulnerable. Annually, hackers are collecting large stores of data from a wide range of industries, but much of that data remains encrypted even after being stolen. Therefore, when hackers are able to execute a breach successfully, they might only obtain indecipherable information that likely can't be translated by a modern computer.[11]

Quantum computers could eventually be used to decrypt this data and expose potentially highly sensitive information stolen in the past. This could implicate a slew of public and private enterprises years, or even decades, after the information was stolen.[12]

Blockchain: Blockchain, initially heralded for its potential to provide ironclad security for everything from cyber currencies to shipping records, has ultimately proven vulnerable to wily hackers.[13] Such blockchain vulnerabilities may only increase if bad actors have quantum computers at their disposal. For example, every transaction that occurs on one blockchain comes accompanied with a public key that's decrypted while the network confirms the block—usually within a period of about ten minutes. This isn't enough time for a classical computer to solve the mathematical equation that unlocks the private key required to access the block, but a quantum computer may be capable of solving that equation in this time frame.[14]

Contributor
David Geller is Emerging Issues Senior Analyst at ISO.

5G Technology

34 5G: New Opportunities and Risks

38 Complex 5G Rollout Comes with Radiation Risks

40 Could 5G Deployment Disrupt Weather Forecasting?

42 How 5G Can Send Drones to New Heights

5G: New Opportunities and Risks

By: Drew Doleski

Technological innovation in both the consumer and enterprise markets continues to drive forward at a blistering pace. Digitization and automation are drastically changing the nature of how society operates, the way we store and access information, how we participate in commerce, how we communicate with others, and how we interact with objects in the physical world.

Next generation 5G wireless networks promise to supercharge these trends. This evolution in wireless is expected to deliver impressive increases in speed and reliability, which will support value creation across nearly all industry sectors. While these benefits will be massively transformative, 5G also has the potential to create new threats that risk managers and the insurance community must account for.

What is 5G?

Fifth-generation wireless, or 5G, is an emerging networking architecture that will increase the speed, efficiency and reliability of data communication compared to fourth-generation (4G) and 4G long-term evolution (LTE) networks. In addition to leveraging new spectrums with increased bandwidth, 5G incorporates advanced radio and software-defined platforms to enable faster data processing needed for virtualization, cloud-based architectures, and edge computing.[1]

If we presume that network speed is the critical benchmark for performance, 5G is poised to deliver a dramatic boost. Presently, fourth-generation LTE has a peak data transfer rate up to 300 megabits per second. While it's still unclear how fast 5G networks will be in production, initial indications point to at least a 3x increase in speed, with some vendors citing gains as high as 20x.[2] In an unscientific test of a consumer-grade 5G-enabled mobile phone, testers saw peak speeds of 1.385 gigabits per second, a nearly 5x boost over 4G LTE.[3]

5G also promises a significant improvement in network latency, reducing response rates in the time a signal is sent to when a reaction begins. This reduction in latency can drastically shift outcomes during life-and-death situations. For example, "a connected car traveling at 75 miles per hour would travel over 10 feet further before applying the brakes if the system experienced a mere 100-millisecond delay," according to VIA Technologies.[4]

In many advanced markets, wireless operators are in the early stages of rolling out 5G infrastructure. This is no small task and involves the participation and coordination of a range of entities including network operators, hardware infrastructure manufacturers, and software providers, and buy-in from the numerous vendors that wish to include 5G radios in their own devices.

5G impact and opportunities

Beyond the projected consumer benefit of speedier wireless devices, the launch of 5G is hotly anticipated as an enabler of many other emerging technologies with widespread impact for numerous industry segments. According to IHS Markit, 5G will create 22 million new jobs globally, generate US $3.5 trillion in direct economic activity and contribute to significant economic growth.[5]

Some areas where the benefits of 5G will be realized include:

- **Connected vehicles:** The next generation of personal and commercial fleets will be built on the promise of enhanced connectivity delivered over 5G. In addition to new opportunities for the delivery of digital services such as predictive maintenance, perhaps the biggest benefit will be vehicle safety. As demand for autonomous and semi-autonomous vehicles grows, so too must a network infrastructure that will support their safe use on roadways. 5G will be a key ingredient in intelligent road infrastructure, such as by optimizing the use of sensors on streetlights that remain in constant communication with autonomous vehicles.

- **Manufacturing:** Many consider automation to be the Fourth Industrial Revolution.[6] This translates to an increase in the use of robotics within manufacturing and the proliferation of Industrial Internet of Things (IIoT) sensors that monitor equipment use and health. The speed, reliability and reduced latency of 5G networks can enhance production controls, help improve worker safety, and increase opportunities for automating a growing number of manufacturing tasks at a significant scale.

- **Healthcare:** Innovations in healthcare will change society's access to medical services and reduce the cost of delivering them. Concepts rolling out today include telemedicine and remote monitoring–all of which benefit from faster, more secure and reliable data sharing between patients and healthcare providers through advanced medical devices.

- **Smart cities and infrastructure:** From mobility to the delivery of utilities, both the public and private sectors are undertaking initiatives to improve the quality of essential services. To fulfill the promise of the smart city, 5G will underpin scalable deployment and management of the many connected devices, sensors, and add-ons necessary to reduce congestion and natural resource consumption. These complex smart city solutions rely on networks that include a massive number of connected devices–spanning vehicles, smart meters, street lights, connected infrastructure, and life safety equipment.

5G and insurance

Just as 3G and 4G cellular connections changed the face of content distribution and commerce, 5G will enable significant opportunities for the Internet of Things (IoT). For example, with more data provided by consumers, and industrial use of IoT devices, insurers may be able to improve risk assessment.

For many insurance carriers, vehicle telematics has already begun to improve the accuracy and sophistication of underwriting personal and commercial auto policies, and 5G will enable support for even more telematics-based data. Similarly, some property insurers have begun to introduce incentives for adding safety-oriented devices such as network-connected water leak sensors, enabling the domain of connected property to grow as well.

As the cost of the technology drops and the reliability improves, manufacturers will have greater incentive to embed sensors that can leverage 5G connections in various products. Commercial and personal insurers alike may soon have access to a greater breadth and depth of risk-related behavioral data collected from the use of these products.

5G will perhaps have an even bigger impact on commercial insurance. Transcending many commercial product lines–from small business owner policies to maritime, cargo, and workers compensation products–access to data from 5G-connected devices can greatly improve the speed and accuracy of providing coverage.

For example, factory employees could have sensors attached to their clothing, enabling the company's workers compensation carrier to identify particularly risky activities that the workers engage in, such as carrying weight with poor posture that lends itself to chronic back injuries. Brokers, underwriters, and risk managers who can harness the power of this information are poised for significant competitive advantage.

5G could usher in a new era of risk

Network operators are bullish on 5G because of the increasing demands for expanded wireless capabilities and utilization. However, given this expected increase in utilization volume, these networks and the data that flows through them also present a potentially significant increase in vulnerabilities that can be exploited. It's paramount that these potential entry points be safeguarded at all levels.

Endpoint-to-endpoint traffic, which requires data packets to move through a range of software systems, could have their own susceptibilities. These risks are exacerbated by the deployment strategy that many

network operators have selected–an evolutionary approach that will rely on existing 4G infrastructure components for cost management.[7] In these instances, 5G may inherit some legacy vulnerabilities from 4G equipment.

A noteworthy consequence of the increased throughput of 5G networks is a reduction in range, thus necessitating more towers in the form of small cells.[8] Each cell, along with the supporting macro-network infrastructure, could be exploited as an entry point for cyber attackers. Further, there's been heated geopolitical debate about the potential for international espionage when many key hardware components are manufactured by companies in other countries.

> "Traditional approaches to cyber security in the 4G world. . .will struggle to defend against the new vulnerabilities introduced in the 5G software stack. . ."

Traditional approaches to cyber security in the 4G world, often built upon reactive incident response and recovery methods, will struggle to defend against the new vulnerabilities introduced in the 5G software stack and must evolve to keep pace with the expected growing use of 5G. By leveraging new tools, including proactive machine learning and artificial intelligence, network and application operators can work to reduce the potential for increasingly complex attack vectors.

Lastly, the proliferation of IoT devices that will be connected to 5G networks represents an exponential growth in risk. Statista forecasts more than 25 billion connected objects by 2025, a nearly 150 percent increase from 2019.[9] Compromised devices, including connected vehicle sensors to components in manufacturing equipment and municipal infrastructure, present the potential for both physical and digital harm. Frequent security patching and real-time authentication are imperative to decrease the exposure to possible exploitation. IoT security researchers are already seeing an 875 percent increase in cyberattacks on network-connected devices between the first half of 2018 and the first half of 2019.[10] While the overwhelming majority of these cyberattacks are considered unsophisticated, they remain a strong indicator that the number of attempted exploitations will only continue to rise as the use of IoT grows.

With the impending global launch of 5G networks and the tremendous growth of connected devices expected in the coming years, risk managers must be prepared to evaluate these new potential entry points for cyber actors and become more proactive in their approaches to cyber security. Data management and security strategies, seamless processes for the safe storage of sensitive information, and compliance with regulatory frameworks and certifications are pivotal to mitigate losses that may grow in both scope and severity.

Despite the potential for increased disruptions and losses, 5G technology will create tremendous new opportunities for value creation, operational efficiency and improvements in our everyday lives. Among other enterprises, insurance carriers can position themselves to incorporate 5G to their advantage, such as collecting more robust data for underwriting and claims-handling sophistication, as well as customer experience differentiation.

Contributor
Drew Doleski is Senior Product Manager, IoT/Telematics, ISO.

Complex 5G Rollout Comes with Radiation Concerns

By: Mark Grossman, Tom Timms, & David Geller

The deployment of fifth-generation cellular networks (5G) is distinct from the first four generations (1G to 4G). For one thing, the capabilities of 5G, which could allow for download speeds 600 times faster than its 4G predecessor,[1] are an unprecedented jump in capacity, performance, and efficiency. But the rollout of 5G does share one thing in common with its predecessors—it has provoked fresh fears about electromagnetic radiation.

5G's need for speed

One reason 5G promises to deliver faster speeds, greater bandwidth, and lower latencies is its high frequency compared with other cellular radiation. However, with higher frequencies comes shorter range, which means that 5G equipment will not be able to deliver signals over long distances and may also struggle to penetrate buildings and other objects.[2]

If a 5G signal is dropped, 4G signals will likely be available to pick up the service. With respect to an individual crossing the street while downloading a movie or browsing a web page, the consequences for this 5G-to-4G handoff are minimal. However, the cutting-edge technology that 5G aims to enable at greater scale, such as autonomous vehicles communicating with each other and doctors performing surgeries remotely through a robot proxy, can't be effectively provided over 4G, making the avoidance of 5G drop-offs vital.

5G radio waves do not travel as far as 4G radio waves. This places the utmost importance on the optimal deployment of the equipment based on area characteristics. The image shows examples of some of the mapping data produced by Geomni UK at a resolution of 2 meters. 4G and earlier technologies typically required a 50 meter resolution level of detail. From a mapping perspective, the challenge is not only to determine the height of each building, but also to include a classification based on building density and use. For example, it is necessary to differentiate between retail parks, complex buildings, and industrial areas, which may have buildings of similar characteristics, but ultimately may have very different network requirements.

A peek behind the 5G buildout

The 5G build-out promises to be massive. It's projected that 300,000 antennas will need to be installed over the course of the build-out in the United States—as many cell towers as have been erected in the last 30 years.[3]

Geomni UK, a Verisk business, provided data for many years to telecom network providers in the United Kingdom to help them plan and develop 3G and 4G networks. Geomni is now providing highly detailed data, derived from imagery and other sources, to support modelling and building of 5G networks. The short waves emitted by 5G equipment make optimal placement imperative to mitigate the chances of drop-offs and interference, making this rollout particularly challenging compared with prior cellular upgrades. Given this, network operators will require more precise and granular maps for 5G installations than for 4G.

Radiation concerns

The short waves of 5G, compared with other cellular frequencies, are not only contributing to operational risks, such as signal drop-offs, but to health concerns as well.

The expectations of a massive 5G-related infrastructure build-out have led to apprehension from some relating to potential radiation risks from the equipment. This isn't unusual. Similar fears also surfaced during the rollout of 2G, 3G, and 4G infrastructure. However, the sheer scale of the equipment involved in 5G may be amplifying worries. In the coming years, one may look out the window in their house and see a 5G cell attached to a nearby streetlight.

> "...research on exposure to 5G frequencies is now focusing on the non-thermal health effects and mechanisms that might cause indirect DNA damage..."

But how real are the radiation risks associated with 5G frequencies? Typically, radiation emitted from devices can be classified into one of two categories: ionizing and non-ionizing. For example, X-ray machines emit ionizing radiation, whereas cell phones and cell phone towers emit non-ionizing radiofrequency (RF) radiation.[4] On a very basic level, ionizing radiation can directly damage DNA and be linked to cancer, whereas non-ionizing RF radiation, which has been deemed safe under typical exposure conditions, can cause heating of tissue but not direct DNA damage. However, research on exposure to 5G frequencies is now focusing on the non-thermal health effects and mechanisms that might cause indirect DNA damage, such as increased oxidative stress or the inhibition of DNA repair mechanisms. For example, a study in Environmental Research[5] painted a scenario in which helical sweat ducts in the skin effectively act as miniature antennas to receive the electromagnetic radiation. The authors of the report concluded that "there is enough evidence to suggest that the combination of the helical sweat duct and wavelengths approaching the dimensions of skin layers could lead to non-thermal biological effects."

It appears that more research is required to ascertain what health effects, if any, there may be from 5G equipment and frequencies. Nevertheless, it seems unlikely that these concerns will deter the buildout of 5G infrastructure in the United States. In 2018, the Federal Communications Commission (FCC) developed a strategy known as the Facilitate America's Superiority in 5G Technology (the 5G FAST Plan),[6] reportedly to assist, in part, in deploying the appropriate infrastructure and making additional spectrum available for 5G services.[7] The march toward 5G is on.

Contributors
Tom Timms is Managing Director of Geomni UK.
Mark Grossman, CIH, CSP, is Manager of Occupational Safety and Health at ISO's Engineering and Safety Service.
David Geller is Emerging Issues Senior Analyst at ISO.

Could 5G Deployment Disrupt Weather Forecasting?

By: John Galantowicz

The fifth-generation cellular network (5G), which may jump-start various industries with its tantalizing speed and minimal latency, could nevertheless deal a setback to a service that's become entrenched in society: weather forecasting.

Underlying every weather forecast is a series of atmospheric measurements and variables that are weighed to make models and predictions. Over time, these models have grown increasingly accurate. In 2019, a five-day forecast was just as accurate as a one-day forecast was in 1980.[1] Additionally, meteorologists have been able to predict Arctic weather events resulting from polar vortex splits more than a month in advance.[2] These capabilities have a wide range of societal benefits, from an individual making weekend plans to a large enterprise keeping tabs on its global supply chains.

However, the measurement technology and weather models that have been refined for years may be threatened by 5G signals that will likely be beaming across the better part of the world within the next decade.

Over the last three decades, satellite measurements of water vapor have proven to be a vital input to weather forecast models. Water moves through the atmosphere in far greater quantities as vapor than as liquid droplets in clouds. The better a forecast model knows the current global water vapor distribution, the more effectively it can forecast clouds, rain, and snow. Satellite water vapor sensing with microwaves at frequencies around 22 to 24 gigahertz (GHz) was pioneered by NASA's NEMS instrument (Nimbus-E Microwave Sounder) that flew in 1972.[3] Since then, advances in sensing technology and forecast model data assimilation have resulted in the steady improvement in forecast capabilities that we take for granted today.

Could weather forecasting prosperity be in jeopardy?

In March 2019, the U.S. Federal Communications Commission (FCC) auctioned off spectrum in the 24 GHz band, which will be used to deliver 5G services.[4] This has attracted the attention of meteorologists because water vapor also emits signals at 23.8 GHz. Scientists, including those with the National Oceanic and Atmospheric Administration (NOAA),[5] are concerned that 5G transmissions at this frequency will drown out the signals produced by water vapor, just as the sun hinders our ability to see the stars in daylight.

The deployment of 5G infrastructure is expected eventually to be ubiquitous, which means that avoiding this interference with the current set of satellite-based instruments is not feasible. Rectifying this would not be straightforward either, as the process of replacing space-based microwave sensing instrumentation could take a decade. New microwave sensing strategies would need to be defined and new sensors built, tested, and launched on future, currently unfunded, satellite missions. Even with new sensors in place, the forecast performance might still fall below current standards.

Working to avoid interference at certain radio frequencies isn't unprecedented for forecasters. However, the magnitude of the 5G interference relative to the water vapor signal and the potential for global usage can render these bands unusable for remote sensing.

The 23.8 GHz spectrum isn't the only radio frequency used for weather forecasting. Weather satellites use multiple ranges to detect weather changes, and it seems future FCC 5G auctions could affect them too. Here are some frequencies that the FCC may auction off in the coming years and how they currently relate to weather forecasting:

- 37.6–38.6 GHz band range, the same range in which rain and snow are measured
- 50.2–50.4 GHz band range, typically considered when measuring atmospheric temperature
- 80–90 GHz range, the same range used to measure clouds and ice[6]

It remains to be seen how this potential spectrum issue will unfold. What is certain, however, is the level of dependency this interconnected and technologically powered world has on accurate weather forecasts.

Why accurate weather forecasts matter

*If weather forecasts regress in effectiveness, there may be a domino effect that spans multiple industries and risks. The **following scenarios** illustrate some of these effects:*

- **Supply chains:** A typhoon is barreling west in the Pacific Ocean and threatens to hit a key supplier located in Southeast Asia in just a few days. However, considerable uncertainty remains as to the trajectory the storm will take, and the supplier is deciding whether to incur the expense and disruption of moving products inland. This would be a costly undertaking, but remaining stationary could lead to catastrophic damages, as well as major disruptions for key customers. Without a reliable weather forecast to guide its decision, the company is essentially rolling the dice.

  Potential risks include: Damages to supplier's product and assets, contingent business interruption (CBI), directors and officers (D&O) claims

- **Storm mitigation:** For three consecutive years, major hurricanes projected to hit Florida missed significantly to the east, causing minimal damage. As a result, frustration ensued from businesses, which lost productivity, and from residents, who were upended from their day-to-day lives for a false alarm. The next year, another hurricane charges toward Florida. About 72 hours before landfall, state regulators again encourage Floridians to brace for the worst, but still jaded from the last few years, the warnings are largely dismissed and ignored. This time around, the Category 4 storm is a direct hit, bringing devastation to property that wasn't properly fortified and to regions that didn't comply with evacuation orders.

  Potential risks include: Damages to buildings, heightened municipal costs, more injuries and casualties contributing to claims, and increased stress on hospitals

- **Commercial transportation:** Trucking, flying, and maritime operations are vital to both domestic and international shipping and trade. All of these are also at the mercy of the weather. A myriad of consequences could result from these enterprises having a shorter window of time to respond to weather forecasts. For example, one shipper might deliver perishables, but an inability to foresee inclement weather could lead to delays and contribute to more frequent spoilage.

  Potential risks include: Damages to trucks, planes, and vessels; damages to cargo; business interruption and contingent business interruption; injuries to employees

Contributor
John Galantowicz is Principal Scientist, Atmospheric and Environmental Research (AER).

How 5G Can Send Drones to New Heights

By: Cory Shelton

This year represented a year of firsts for the drone industry, reaching multiple milestones that could pave the way for more ubiquitous use in the future.

For instance, the Federal Aviation Administration (FAA) approved operations for a revenue-generating drone delivery service for the first time, permitting UPS to pair up with Matternet, an autonomous delivery drone startup, to deliver medical supplies in Raleigh, North Carolina.[1] The venture is projected to allow for transport of potentially life-saving samples to be delivered in 3 minutes and 15 seconds, a steep drop from the 30 minutes typically needed to deliver through car traffic in the same range.[2]

> "Future air traffic control systems… could access real-time data…allowing for an ecosystem that could prevent collisions."

The FAA also, for the first time, certified a drone delivery company as an air carrier, citing the company's ability to demonstrate compliance with strict FAA safety requirements.[3]

Certainly, this represents progress for an industry that has yet to fully take off. To make even greater strides in the coming years, technology will need to be developed to cultivate an Unmanned Aircraft System Traffic Management (UTM) system that can complement the FAA's Air Traffic Management (ATM) system.[4] UTM is the missing puzzle piece to a nationwide airspace network that would allow for drones, helicopters and fixed-wing aircraft to live in harmony and, more important, not collide with one another.

There is optimism building that 5G, with its rapid speeds and minimal latency, will facilitate the development of a more optimal UTM.

How the 4G to 5G evolution will affect drones

- **Improved traffic systems:** Currently, the biggest issue with creating a viable traffic management system for drones involves their limited connectivity to the Internet. The vast majority of drone systems currently available establish only a local connection to the ground station. At no time does the drone directly connect to the Internet itself.

  Without this Internet connection, a drone might not be able to broadcast its current position and altitude, which could lead to mid-air collisions.

This issue could be rectified by embedding 5G transmitters into drones. If integrated, the transmitters will allow drones to connect to the network, enabling them to broadcast their location and receive instructions from the cloud. With these transmitters, future air traffic control systems and other aircrafts could access real-time data on the drone, allowing for an ecosystem that could prevent collisions.

- **Increased bandwidth:** Drones that operate within the 5G network will also benefit from the same bandwidth typically provided by most cable or fiber-optic connections, enabling a host of new drone-based services.

  With the increased bandwidth, drones may be able to beam the Internet to remote and underserved areas. Additionally, in time, drones could stream 4K or even 8K video across the globe with only a few milliseconds of latency.

Drone risks of the future

Increased tracking capability and other safety measures could mean more prevalent drone use, but with increased use comes increased risk. Here are a couple of potential issues that could arise as drone use surges:

- **Loss of connection:** While the improvement of Unmanned Aircraft Systems Traffic Management (UTM) systems and other drone technology is alleviating fears about drone-related incidents, some questions remain. Contemporary drones typically use a basic form of Return To Launch (RTL) function, which essentially sets a geolocated home point that the drone will return to for landing in case of a loss of connection. But what happens when a delivery drone attempts to navigate a large metropolitan city and the 5G transmitter fails or the Internet goes out? If a drone loses connection with its pilot several miles away, how will it navigate autonomously in a dense urban city flooded with other airborne objects and tall buildings? Ultimately, refining any nascent technology can be difficult because the real-world presents a variety of potential unforeseen circumstances. Drones appear to be no exception to this.

- **Privacy:** By virtue of 5G-enabled fleets of drones patrolling skies regularly, their cameras and sensors will inherently be able to collect troves of data unlikely to be destroyed once aggregated to a database. The incorporation of facial recognition into both public and private enterprises was a prominent theme in 2019, and there have been reports of some drones already being equipped with this technology as well.[5] Additionally, similar to home smart speakers reportedly collecting and keeping audio unbeknownst to some users, drones may also be able to pick up and keep footage of individuals without their consent. The possibility of this footage being breached could lead to the revelation of addresses, whereabouts, and other highly personal information.

Contributor
Cory Shelton is Director of UAV Services, Geomni.

Cannabis

46 How Bioengineering Could Reshape the Cannabis Industry

49 As Market for CBD Products Blooms, Questions Grow around Human Safety

How Bioengineering Could Reshape the Cannabis Industry

By: Thad Nosal, Hans Plugge, and David Geller

Marijuana is a risky business. Whether in the cultivation, manufacturing, or processing stage, businesses engaged with the industry face a laundry list of potential pitfalls.

For instance, the electricity and infrastructure typically required to foster the hot, humid, carbon dioxide–rich environment needed to grow cannabis can result in a litany of risks that includes mold and explosions.

Additionally, a dearth of research substantiating the type and quantity of pesticides needed in cannabis farming has resulted in a lack of adequate information around the safe use of pesticides in cannabis cultivation, thus increasing the potential for unsafe or contaminated cannabis products being sold to the public. As a result of continuing regulatory restrictions, crop rotation as a method of pest control cannot be practiced.[1]

These, as well as other factors, have made the growing field of cannabis bioengineering a potentially more appealing long-term source for producing cannabis compounds. Bioengineering includes the modification of the plant itself and the development of microorganisms modified to produce cannabis compounds.[2]

How bioengineering cannabis compounds can reduce risk

In 2019, researchers published a study in which brewer's yeast was bioengineered to produce cannabidiol (CBD) and tetrahydrocannabinol (THC), demonstrating the efficacy of bioengineering as a tool to produce cannabis compounds.[3] At least 12 companies are considering using bioengineering to produce cannabis compounds without the need to grow cannabis plants.[4]

If scalable, producing cannabis compounds using bioengineering could address risks inherent in traditional cultivation, such as:

- **Making product development more environmentally sustainable:** Not only could bioengineering limit the need for hazard-laden greenhouses, it could also consume less energy and water, thus aligning with worldwide sustainability goals to limit emissions and respond to growing water scarcity.[5]

- **Reducing dangerous by-products:** This technique could address a problem that emerges from the process of extracting specific compounds from a cannabis plant. On occasion, CBD extracts or fractions, which are composed of multiple components, have retained some THC in the final products.[6] Given the increasingly prevalent use of CBD for wellness products, even a trace amount of the psycho-active THC within these products could be a cause for concern, especially if children are using products infused with cannabis compounds.

  This issue could be resolved using bioengineering, since marijuana manufacturers could bypass working with the marijuana plant, thus enabling the production of pure cannabis components that should not contain any unintended extracts.

How bioengineering cannabis compounds opens new doors

More than 500 chemicals have been identified in cannabis, including over 100 different cannabinoids. Cannabinoids are chemicals that interact with the body's endocannabinol system to trigger physiological reactions. With respect to cannabinoids, CBD and THC tend to be discussed most often, but other cannabis compounds have exhibited properties that have piqued the interest of scientists.[7]

> "At least 12 companies are considering using bioengineering to produce cannabis compounds without the need to grow cannabis plants."

The limited presence of these minor compounds in the cannabis plant has restricted the ability to research such compounds in-depth. Bioengineering allows for the mass production of these more obscure molecules, thus allowing for more in-depth study.[8]

These compounds can be created using bioengineered yeast, algae, and bacteria. Bioengineering has been prominently used in the past for other products, such as insulin, which became scalable after using yeast to produce much higher quantities at a lower price. Also, biosynthesis offers the possibility of producing individual compounds at higher purity than could be achieved from extracting the chemicals from plant material.[9]

Cannabinoids aren't the only part of the cannabis plant that may entice more research. A study in the 1980s remarked that Cannflavin A and Cannflavin B, two flavonoids within the cannabis plant, have anti-inflammatory properties that are 30 times more powerful than aspirin. However, these flavonoids comprise merely .014 percent of the fresh weight of the marijuana plant, making extraction considerably difficult and thus limiting research.[10]

Bioengineering could allow for these components to be mass-produced and enable scientists to research their properties and potential benefits.

Risky business: A world with more cannabis products could be on the horizon

Harnessing cannabis for further medical use and treatment is enticing. However, the introduction of new cannabinoids and cannabis components into the market could trigger the same issues as the burgeoning CBD market, such as potential regulatory confusion and misrepresentations in advertising.[11]

Additionally, one area of research that's still ambiguous is how different cannabinoids interact with each other and how that may affect human health after consumption. If more cannabinoids (CBN, for example) or other components are mass-produced, then it isn't difficult to envision a scenario in which an individual is ingesting CBD and CBN for different purposes, such as anxiety and sleep assistance, as well as THC for recreational use.

This quandary was alluded to at a June 2019 Federal Drug Administration (FDA) hearing involving CBD. The FDA Commissioner asked, in part, how CBD would interact with other drugs an individual might be taking.[12] Of note, some researchers in the past have expressed concern that CBD could cause issues with blood thinning medication. For example, CBD could block the metabolism of warfarin, which might enable it to stay in the system longer, potentially leading to toxicity or a traumatic bleed or dangerous hemorrhage.[13] Additionally, a review published subsequent to the meeting identified several classes of medications that may be affected by concurrent use with CBD.[14]

Other compounds and cannabinoids

As noted earlier, there are more than 500 chemicals and at least 100 cannabinoids in cannabis, among them CBD and THC. While research on many of these compounds is scarce, here are some to keep an eye on.

Cannabinol (CBN): CBN is reported to be similar in chemical composition to THC and is thought to be mildly psychoactive. There's a belief that its operation as an agonist to the TRPV2 receptor can make it potentially effective for mitigating pain and inflammation, lowering blood pressure, and treating skin conditions.[15] It's also being investigated as a potential sleep aid,[16] which is noteworthy because 50 to 70 million Americans have a sleep disorder, according to the American Sleep Association (ASA).[17]

Tetrahydrocannabinol acid (THC-A): This is the component that when heated is converted to THC, a cannabinoid that produces psychoactive effects.[18] Potential benefits that THC-A may offer include anti-inflammatory properties, relief for nausea and vomiting, and possible treatment for neurogenerative disorders.[19,20]

Cannabigerol (CBG): Cannabigerol's potential is drawing attention, in part due to a preliminary study in which CBG ingestion led to the creation of new brain cells in mice,[21] displaying similar potential as THC-A to treat neurogenerative disorders. Additionally, this cannabinoid is being identified as a possible compound to fight cancer, showing the ability to block receptors that contribute to cancer cell growth.[22]

Contributors
Thad Nosal, Director, Engineering and Safety Service, ISO.
Hans Plugge, Senior Toxicologist and Manager, Safer Chemical Analytics, Verisk 3E.
David Geller is Emerging Issues Senior Analyst at ISO.

As Market for CBD Products Blooms, Questions Grow around Human Safety

By: Patricia Iscaro

What do you think of when you hear the word cannabis? For some readers, their thoughts may drift to media reports proclaiming the legalization of recreational marijuana in several U.S. states. But the market for cannabis-based products reaches far beyond recreational marijuana. Indeed, it's possible that several cannabis-based products are being sold currently in a pharmacy near you. And recent regulatory changes may open the door for an even wider influx of cannabis-based products in the future.

The question is: How safe are these products and what risks do they pose for insurers?

The explosive growth of cannabidiol

One major growth market for cannabis is products containing cannabidiol, or CBD. As the name suggests, cannabidiol is an active ingredient derived from cannabis—specifically, the Cannabis sativa L. plant, including hemp and marijuana.[1] CBD is generally sourced from hemp, not marijuana, since hemp usually contains 0.3 percent or less of THC, the psychoactive molecule that imparts the "high" associated with marijuana consumption.

Industry research indicates that sales of CBD-based products have increased 706 percent since 2018 and are expected to surge to more than a US $5 billion industry by the end of 2019.[2] By 2022, industry researchers believe the market could soar to US $22 billion.[3] This product boom includes everything from tinctures to vape oil and edibles such as gummies and syrup. Not surprisingly, hemp farming is also a growth market. According to data gathered by the advocacy group Vote Hemp, from 2018 to 2019 hemp acreage under license in the United States grew 511,442 acres, an increase of 476 percent.[4]

How is hemp regulated?

What's fueling the growth of this cash crop? In part, it's a new regulatory regime ushered in by state legislatures and, at the federal level, by the 2018 U.S. Agricultural Improvement Act, aka the 2018 Farm Bill.[5]

The 2018 Farm Bill generally changed the status of hemp from a controlled substance regulated under the Controlled Substances Act (CSA) to a substance subject to Food and Drug Administration (FDA)-regulatory requirements.[6] It did so by removing hemp and derivatives of cannabis with no more than 0.3 percent THC concentration on a dry weight basis from the CSA's definition of marijuana.[7]

While no longer a controlled substance, hemp and cannabis derivatives with 0.3 percent or lower THC concentrations are still regulated. As explained by the FDA, "FDA treats products containing cannabis or cannabis-derived compounds as it does any other FDA-regulated products—meaning they're subject to the same authorities and requirements as FDA-regulated products containing any other substance."[8]

> "It remains an open question as to how…pesticide concentrations might affect users who ingest and inhale cannabis-based products like CBD."

The FDA has generally concluded it is illegal under federal law to add CBD to food or market it as a dietary supplement.[9]

Related federal prohibitions have not stopped some states, such as New Mexico, from passing laws that generally allow for the incorporation of hemp-derived CBD in food products.[10] Nor has it deterred some manufacturers from producing and selling food products containing CBD. To date, the FDA has sent warning letters to several companies using disease-curing claims to market their CBD products.[11] But products proclaiming the supposed stress relieving and anti-inflammatory benefits of CBD (among other claims) remain in circulation.

Concern about CBD product safety

The FDA has highlighted a number of health and safety concerns with respect to the budding market for CBD products and has published a list of its more pressing concerns around CBD product safety, including:[12]

- the long-term effects of regularly ingesting CBD
- the cumulative exposure to CBD through a variety of products. (What happens if you eat food with CBD in it, use CBD-infused skin cream and take other CBD-based products on the same day? What if you use these products daily for a week or a month?)
- the effects of CBD on special populations such as the elderly, children, adolescents, and pregnant and lactating women
- the safety of CBD use in animals and pets

In Senate testimony on July 25, 2019, an FDA official highlighted another concern, noting that laboratory analysis of some of CBD products revealed they did not contain the amount of CBD stated on a product's label, and/or the products contained other substances that were not on the product's label, such as other cannabinoids like THC.[13]

Pesticides used in growing hemp

In addition to these concerns, there's also the issue of pesticides used in the production of hemp. The U.S. Environmental Protection Agency (EPA) generally regulates pesticide use in agriculture, along with state and local jurisdictions. As of authoring, there are currently no pesticides registered by the EPA specifically for use on cannabis, although applications requesting the expanded use of registered pesticide products for hemp are currently in review. Consequently, there are no tolerances established for hemp to be used for food/supplements.[14]

With CBD products proliferating onto store shelves, researchers are concerned about the potential for high concentrations of pesticides in CBD products that are ingested or inhaled. That's because unlike some crops, cannabis can be dried or turned into oils thereby concentrating any chemicals or pesticides used on the plant. It remains an open question as to how those pesticide concentrations might affect users who ingest and inhale cannabis-based products like CBD.[15]

An evolving market

As the cannabis industry continues to grow, legislatures will need to keep up and regulatory agencies will need to promulgate regulations to ensure consistent standards for cultivation and consumer safety. Insurers, too, will need to pay keen attention to the dynamics of this market as it promises to impact everything from general and product liability coverages and beyond.

Contributor
Patricia Iscaro is Manager of the Americas for Regulatory Research, Verisk 3E.

About Verisk Business Units

AER Atmospheric and Environmental Research (AER) provides science-based solutions to global environmental challenges. AER's internationally renowned scientists and software engineers collaborate to transform state-of-the-art predictive science and analytical tools into practical systems that address both civilian government and defense needs for geophysical understanding, computer simulation, and forecasting. AER customers include government agencies and national laboratories, aerospace and defense contractors, and academia. Areas of expertise comprise atmospheric and environmental science, remote sensing, meteorology, oceanography, space science, climate change, and software engineering. AER was established in 1977 and is headquartered in Lexington, Mass. Visit **www.aer.com**.

AIR Worldwide AIR Worldwide provides risk modeling solutions that make individuals, businesses, and society more resilient to extreme events. In 1987, AIR Worldwide founded the catastrophe modeling industry and today models the risk from natural catastrophes, terrorism, pandemics, casualty catastrophes, and cyber incidents. Insurance, reinsurance, financial, corporate, and government clients rely on AIR's advanced science, software, and consulting services for catastrophe risk management, insurance-linked securities, longevity modeling, site-specific engineering analyses, and agricultural risk management. AIR Worldwide is headquartered in Boston, with additional offices in North America, Europe, and Asia. For more information, please visit **www.air-worldwide.com**.

Geomni Geomni uses remote sensing and machine learning technologies to capture, store, process and deliver the most accurate aerial imagery and geospatial data. Our data analytics and imagery solutions serve a variety of industries including P&C insurance, construction, engineering firms, government, urban planning, utilities, and more. Mapping professionals leverage our extensive aerial intelligence to better understand growth and change, detect damage, find hazards, assess risk and perform valuations. In a nutshell: We enable you to make more informed, data-driven decisions. Visit: **www.geomni.com**.

ISO ISO is a Verisk business, is a leading provider of advanced tools and analytics for the property/casualty insurance industry. Drawing on unique data assets and deep domain expertise, ISO products and services help insurers underwrite and price risks with greater precision and efficiency and manage claims more effectively across the spectrum of commercial and personal lines of insurance. For more information, visit **www.verisk.com/iso**.

Verisk 3E Verisk 3E, formerly 3E Company, delivers intelligent compliance solutions that empower companies to reduce risk, drive continuous improvement, and create new growth opportunities. For 30 years, Verisk 3E has provided clients with the expertise, content, live 24/7/365 environmental health and safety (EHS) support, and award-winning solutions required to increase chemical and workplace safety, improve product safety and stewardship, strengthen supply chain stewardship, and optimize research and development decision support. Visit: **www.verisk3e.com**.

Verisk Maplecroft For over 10 years, Verisk Maplecroft has pioneered the quantification of risk. Our journey has seen us become part of the world's leading data analytics organization and progress from a team of talented academics based in the west of England to a global research house at the forefront of data modelling, risk analysis, and forecasting. Visit: **www.maplecroft.com**.

Wood Mackenzie Wood Mackenzie is a trusted source of commercial intelligence for the world's natural resources sector. We empower clients to make better strategic decisions, providing objective analysis and advice on assets, companies and markets. Visit: **www.woodmac.com**.

Learn More About ISO Emerging Issues

Interested in jumpstarting your research efforts for risks affecting your business, or keeping tabs on a risk you're already monitoring?

The ISO Emerging Issues team covers more than 40 emerging risks and trends to help you do just that. Visit **www.verisk.com/ei** to access the Emerging Issues research website to explore these insights, as well as subscribe to a weekly newsletter that provides freshly authored content drafted in response to the latest news and developments.

ISO Emerging Issues Team

William Mauro

Billy Mauro is the senior director of commercial casualty product development at ISO. In this role, he leads teams helping develop ISO casualty coverage initiatives, including those related to general liability, commercial auto, commercial umbrella/excess, businessowners, and medical professional liability, premium audit advisory services, and insurance case law research. Over his 16 years with ISO, he has contributed to ISO work in a number of areas, including home healthcare, construction defects, liquor liability, data breach exposures, and additional insureds. Billy also leads the ISO Emerging Issues unit. He has contributed articles to several insurance publications and is a frequent presenter at industry events.

Andrew Blancher

Andrew Blancher, CPCU is director of both commercial automobile product development and emerging issues at ISO. Andrew is responsible for overseeing the development, revision, and maintenance of ISO's commercial automobile forms, rules, and loss costs programs. He has more than 30 years of experience in commercial automobile insurance. As director of emerging issues, Andrew manages a research team that analyzes a host of technological, atmospheric, and societal changes and publishes timely content contextualized for the insurance industry. Andrew has authored numerous articles for Verisk and trade publications. He is a frequent guest speaker and panelist at industry conferences and a teacher at accredited educational seminars.

Christopher Sirota

Christopher Sirota, CPCU is Emerging Issues product development lead at ISO. Christopher is responsible for research in emerging risks that may affect the insurance industry to support product development and for maintaining the ISO Emerging Issues website. With almost 20 years at ISO, Christopher has previously been involved in product development for personal and commercial auto programs related to telematics and connected vehicles. He also has presented at industry events on the topic.

David Geller

David Geller, CPCU, SCLA is Emerging Issues senior analyst at ISO. David is responsible for research in emerging risks that may affect the insurance industry to support product development, and to maintain the ISO Emerging Issues website. David has presented at industry events on a variety of emerging issues. David has helped develop new ISO commercial programs as well as file revised state endorsements in response to regulatory developments. Prior to joining ISO, David was a liability claims examiner and commercial lines underwriter.

Polar Vortex Splits Causing Major Disruption

1. Cohen, Judah. “Splitting the Polar Vortex: Is the Earth Spinning the Wrong Way?” Verisk.com. March 9. 2018. https://www.verisk.com/insurance/visualize/splitting-the-polar-vortex-is-the-globe-spinning-the-wrong-way/
2. Roach, John. “Polar Vortex’s Bitter Cold Could Cost U.S. Economy $5 Billion, Though the Worst May Be Over.” AccuWeather.com. July 8, 2019. https://www.accuweather.com/en/weather-news/polar-vortexs-bitter-cold-could-cost-us-economy-5-billion-though-the-worst-may-be-over/70007309
3. Nace, Trevor. “Greeland Lost 12.5 Billion Tons of Ice In a Day, a Grave Reminder of Our Changing Planet.” Forbes.com August 6, 2019. https://www.forbes.com/sites/trevornace/2019/08/06/greenland-lost-125-billion-tons-of-ice-in-one-day-a-grave-reminder-of-our-changing-planet/#4591882c3986
4. Sousounis, Peter. “Can ‘Global Warming’ Cause More Wintry Conditions? Air-Worldwide.com March 29, 2018. https://www.air-worldwide.com/Blog/Can-%E2%80%9CGlobal-Warming%E2%80%9D-Cause-More-Wintry-Conditions-/

Sea Level Change: Examining Hot Spots and Their Potential Implications for Insurance and Society

1. Hallegatte, S., Green, C., Nicholls, R.J., and Corfee-Morlot, J. (2013). “Future flood losses in major coastal cities.” Nature Climate Change, 3(9), 802–806. https://doi.org/10.1038/nclimate1979
2. Kopp, R.E, Gilmore, E.A., Little, C.M, Lorenzo-Trueba, J., Ramenzoni, V.C., and Sweet, W.V. “Sea-level science on the frontier of usability.” In press in Earth’s Future

Where Climate Change and Natech Risk Meet

1. Rasmussen, K., 1995. Natural events and accidents with hazardous materials. J. Hazard. Mater. 40, 43–54.
2. Sengul, H., Santella, N., Steinberg, L.J., Cruz, A.M., 2012. Analysis of hazardous material releases due to natural hazards in the United States. Disasters, 36, 723–743
3. France-Presse, A., 2016. Outrage as plant bosses acquitted over fatal toxic spill in Hungary. The Guardian. Available at: https://www.theguardian.com/world/2016/jan/28/outrage-plant-bosses-acquitted-fatal-toxic-spill-hungary. Accessed: 11th October 2019.
4. Santella, N., Steinberg, L.J., Sengul, H., 2010. Petroleum and Hazardous Material Releases from Industrial Facilities Associated with Hurricane Katrina. Risk Anal. 30, 635–649.
5. Sengul, H., Santella, N., Steinberg, L.J., Cruz, A.M., 2012. Analysis of hazardous material releases due to natural hazards in the United States. Disasters, 36, 723–743
6. Hoffman, R. N., Dailey, P., Hopsch, S., Ponte, R. M., Quinn, K., Hill, E., Zachry, B., 2010. An Estimate of Increases in Storm Surge Risk to Property from Sea Level Rise in the First Half of the Twenty-First Century, Weather, Climate, and Society, 2, 271-293.

Power Utilities Face Emerging Cyber Threats

1. “Industrial Control Systems Are Still Vulnerable to Malcious Cyberattacks.” MIT Technology Review.com. January 28, 2019. https://www.technologyreview.com/s/612829/industrial-control-systems-are-still-vulnerable-to-malicious-cyberattacks/
2. Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” Wired.com March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
3. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.”
4. “AMI Global Forecast 2019-2024: H1 2019.” Woodmac.com July 11, 2019. https://www.woodmac.com/reports/power-markets-ami-global-forecast-2019-2024-h1-2019-325635
5. Pagliery, Jose. “Sniper Attack on California Power Grid May Have Been ‘an Insider,’ DHS Says.” CNN.com. October 17, 2015. https://money.cnn.com/2015/10/16/technology/sniper-power-grid/index.html
6. Baker, David R. “FBI: Attack on PG&E South Bay Substation Wasn’t Terrorism.” SFGate.com. September 11, 2014. https://www.sfgate.com/business/article/FBI-Attack-on-PG-amp-E-substation-in-13-wasn-t-5746785.php
7. Chappell, Carmin. “Saudi Arabia Reportedly Aims to Restore One Third of Lost Oil Output by Monday.” CNBC.com.September 15, 2019. https://www.cnbc.com/2019/09/15/saudi-arabia-aims-to-restore-one-third-of-lost-oil-output-by-monday-wsj-says.html
8. “Global Oil Markets Reminded of Supply Vulnerability.” Woodmac.com, September 16, 2019. https://my.woodmac.com/reports/oil-markets-global-oil-market-reminded-of-supply-vulnerability-347025

Cyber Risks Loom Large in an Interconnected World

1. “Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks.” Businesswire.com. November 15, 2018. https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-2018-Third-Party
2. “Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks.”
3. Boyens, Jon. “Integrating Cybersecurity into Supply Chain Risk Management.” RSAConference.com February 29, 2016. https://www.rsaconference.com/writable/presentations/file_upload/grc-w03_integrating_cybersecurity_into_supply_chain_risk_management.pdf
4. Or-El, Matan. “Supply Chain Cybersecurity Is One of the Biggest Issues Facing Logistics Planners.” InboundLogistics.com. February 28, 2019. https://www.inboundlogistics.com/cms/article/the-abcs-of-supply-chain-cybersecurity/
5. Whittaker, Zack. “Researchers Find 540 Million Facebook User Records on Exposed Servers.” TechCrunch.com. April 3, 2019. https://techcrunch.com/2019/04/03/facebook-records-exposed-server/
6. McGrath, Maggie. “Target Data Breach Spilled Info On As Many as 70 Million Customers.” Forbes.com. January 10, 2014. https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#3186030fe795

7. Krebs, Brian. “Target Hackers Broke in Via HVAC Company.” KrebsOnSecurity.com. February 14, 2019. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
8. “Cost of 2013 Target Data Breach Nears $300 Million.” TheSSLStore.com. May 26, 2017. https://www.thesslstore.com/blog/2013-target-data-breach-settled/
9. “Norsk Hydro Cyber Attack Cost It Nearly $52M In First Quarter.” InsuranceJournal.com. April 30, 2019. https://www.insurancejournal.com/news/international/2019/04/30/525093.htm
10. O’Byrne, Rob. “Supply Chains and the Internet of Things—Towards New Paradigms.” LogisticsBureau.com. March 6, 2018. https://www.logisticsbureau.com/supply-chain-the-internet-of-things-towards-new-paradigms/

Cybersecurity Needs a Quantum Leap

1. Beall, Abigail & Reynolds, Matt. “What Are Quantum Computers and How Do They Work? WIRED Explains.” Wired.com. February 2018. https://www.wired.co.uk/article/quantum-computing-explained
2. Simonsen, Scott. “Quantum Communication Just Took a Great Leap Forward.” SingularityHub.com. December 26, 2018. https://singularityhub.com/2018/12/26/quantum-communication-just-took-a-great-leap-forward/#sm.0001fg5v81cn3fhdt3l2gzub5ml5f
3. Prisco, John. “The United States Needs a Better Quantum Science as a National Policy.”TheHill.com. December 6, 2018. http://thehill.com/opinion/technology/419810-the-united-states-needs-better-quantum-science-as-a-national-policy
4. “How a Quantum Computer Could Break 2048-bit RSA Encryption in 8 Hours.” MIT Technology Review.com. May 30, 2019. https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/
5. “How a Quantum Computer Could Break 2048-bit RSA Encryption in 8 Hours.”
6. Takashi, Dean. “IBM Research explains how quantum computing works and why it matters.” VentureBeat.com. July 14, 2019. https://venturebeat.com/2019/07/14/ibm-research-explains-how-quantum-computing-works-and-could-be-the-the-supercomputer-of-the-future/
7. Grody, Allan. “We Aren’t Prepared for the Next Wave of Cyber Risks.” TheHill.com. April 7, 2019. https://thehill.com/opinion/cybersecurity/437739-we-arent-prepared-for-the-next-wave-of-cybersecurity-risks
8. Mandelbaum, Ryan F. “You Won’t See the Quantum Internet Coming.” Gizmodo.com. August 21, 2019. https://gizmodo.com/you-wont-see-quantum-internet-coming-1836888027
9. Moody, Dustin. “Updated on the NIST Post-Quantum Cryptography Project.” Csr.nist.gov. https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2_post-quantum_dmoody.pdf
10. Herman, Arthur. “The Quantum Revolution Is Coming, Ready or Not.” Forbes.com. March 12, 2019. https://www.forbes.com/sites/arthurherman/2019/03/12/the-quantum-revolution-is-coming-ready-or-not/#4d8c24a265a3
11. Mims, Christopher. “The Day When Computers Can Break All Encryption Is Coming.” WSJ.com. June 4, 2019. https://www.wsj.com/articles/the-race-to-save-encryption-11559646737
12. “The Day When Computers Can Break All Encryption Is Coming.”
13. Orcutt, Mike. “Once Hailed As Unhackable, Blockchains Are Now Getting Hacked.” MITTechnologyReview.com. February 19, 2019. https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/
14. Stevens, Robert. “Bitcoins Race to Outrun the Quantum Computer.” Finance.Yahoo.com. August 21, 2019. https://finance.yahoo.com/news/bitcoin-race-outrun-quantum-computer-133902176.html

5G: New Opportunities and Risks

1. “What Is 5G?” Cisco.com. https://www.cisco.com/c/en/us/solutions/what-is-5g.html
2. Khairy, Mohammed Al. “5G: Your Life Is About to Change.” Qualcomm.com October 29, 2018. https://www.qualcomm.com/news/onq/2018/10/29/5g-your-life-about-change
3. Swider, Matt. “5G Speed Test: 1.4Gbps in Chicago, but Only If You Do the ‘5G Shuffle.’” TechRadar.com. May 19, 2019. https://www.techradar.com/news/5g-speed-test
4. “As 5G Networks Prepare for Launch in Early 2019, 5G Technology and Fog Computing are the Intelligent Network Architecture of the (Near) Future.” Viatech.com. January 2, 2019. https://www.viatech.com/en/2019/01/5g-edge-ai-powering-fog-computing/
5. “The Promise and Potential of 5G: Evolution of Revolution?” IHSmarkit.com. April, 2019. https://cdn.ihs.com/www/pdf/0419/IHS-Markit-Technology-5G-The-Promise-Potential.pdf
6. McGinnis, Devon. “What Is the Fourth Industrial Revolution?” Salesforce.com. December 20, 2018. https://www.salesforce.com/blog/2018/12/what-is-the-fourth-industrial-revolution-4IR.html
7. Grijpink, Ferry; Menard, Alexandre; Sigurdsson, Halldor & Vucevic, Nemanja. “The Road to 5G: The Inevitable Growth of Infrastructure Cost.” Mckinsey.com. February 2018. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-road-to-5g-the-inevitable-growth-of-infrastructure-cost
8. Rajiv. “What Are Small Cells in 5G Technology.” Rfpage.com. September 5, 2018. https://www.rfpage.com/what-are-small-cells-in-5g-technology/
9. Holst, Arne. “Global Industrial/Consumer IoT Connected Objects 2018-2025.” Statista.com. May 24, 2019. https://www.statista.com/statistics/976079/number-of-iot-connected-objects-worldwide-by-type/
10. Bayern, Macy. “Kaspersky Honeypots Find 105 Million Attacks on IoT Devices in First Half of 2019.” Techrepublic.com. October 15, 2019. https://www.techrepublic.com/article/kaspersky-honeypots-find-105-million-attacks-on-iot-devices-in-first-half-of-2019/

Complex 5G Rollout Also Comes with Radiation Concerns

1. Finley, Klint. “The WIRED Guide to 5G.” Wired.com. December 13, 2018. https://www.wired.com/story/wired-guide-5g/
2. Chandler, Nathan. “5G and Millimeter Wave Tech.” HowStuffWorks.com. https://electronics.howstuffworks.com/5g3.htm
3. ”5G Service Is Coming—And So Are Health Concerns Over the Towers That Support It.” CBSNews.com. May 29, 2018. https://www.cbsnews.com/news/5g-network-cell-towers-raise-health-concerns-for-some-residents/
4. Belluz, Julia. “A Comprehensive Guide to the Messy, Frustrating Science of Cellphones and Health.” Vox.com. November 2, 2018. https://www.vox.com/2018/7/16/17067214/cellphone-cancer-5g-evidence-studies
5. Betzalel, N., Ben Ishai, P., Feldman, Y., 2018. “The human skin as a sub-THZ receiver – Does 5G pose a danger to it or not?” Environmental Research
6. ”The FCC’s 5G FAST Plan.” FCC.gov. September 28, 2018. https://www.fcc.gov/document/fccs-5g-fast-plan
7. The FCC’s 5G FAST Plan.”

Could 5G Deployment Negatively Affect Weather Forecasting?

1. Alley, Richard B., Emanual, Kerry A., Zhang, Fuqing. “Advances in Weather Prediction.” Sciencemag.org. January, 25, 2019. https://science.sciencemag.org/content/363/6425/342
2. Meyer, Robinson. “Modern Weather Forecasts Are Stunningly Accurate.” TheAtlantic.com. January 30, 2019. https://www.theatlantic.com/science/archive/2019/01/polar-vortex-weather-forecasting-good-now/581605/
3. BARNETT, J., HOUGHTON, J., MORGAN, C. et al. Stratospheric Observations from Nimbus 5. Nature 245, 141–143 (1973) doi:10.1038/245141a0
4. Hart, Kim, Freedman, Andrew. “5G Spectrum and the Potential Weather Forecasting Apacolypse.” Axios.com. May 23, 2019. https://www.axios.com/5g-spectrum-and-the-potential-weather-forecasting-apocalypse-1f531685-fc42-4b15-b06a-2e3e6f58210c.html?
5. “5G Spectrum and the Potential Weather Forecasting Apocalypse.”
6. Niiler, Eric. “5G Networks Could Throw Weather Forecasting into Chaos.” Wired.com. May 17, 2019. https://www.wired.com/story/5g-networks-could-throw-weather-forecasting-into-chaos/

How 5G Can Send Drones to New Heights

1. Hawkins, Andrew. “UPS Will Use Drones to Deliver Medical Supplies in North Carolina.” Vox.com. March 26, 2019. https://www.theverge.com/2019/3/26/18282291/ups-drone-delivery-hospital-nc-matternet
2. Premack, Rachel. ”UPS just beat out Amazon, FedEx, and Uber to make America’s first revenue-generating drone delivery.” BusinessInsider.com. March 26, 2019. https://www.businessinsider.com/ups-first-revenue-generating-drone-delivery-with-matternet-2019-3
3. “U.S. Transportation Secretary Elaine L. Chao Announces FAA Certification of Commercial Package Delivery.” FAA.gov. April 23, 2019. https://www.faa.gov/news/press_releases/news_story.cfm?newsId=23554
4. “Unmanned Aircraft System Traffic Management. (UTM.” FAA.gov. February 1, 2019. https://www.faa.gov/uas/research_development/traffic_management/
5. Brad. “Seven Best Drones with Facial Recognition.” TheDroidGuy.com. October 9, 2019. https://thedroidguy.com/2019/09/7-best-drones-with-facial-recognition-1077684

How Bioengineering Could Reshape the Cannabis Industry

1. Holmes, Mowgli, Voelker, Rodger. “Pesticide Use on Cannabis.” CannabissSafetyInstitute.org. June 2105. http://cannabissafetyinstitute.org/wp-content/uploads/2015/06/CSI-Pesticides-White-Paper.pdf
2. Dolgin, Elie. “The Bioengineering of Cannabis.” Nature.com. August 28, 2019. https://www.nature.com/articles/d41586-019-02525-4
3. Sanders, Robert. “Yeast Produce Low-Cost, High-Quality Cannabinoids.” ScienceDaily.com. February 27, 2019. https://www.sciencedaily.com/releases/2019/02/190227131838.htm
4. “The Bioengineering of Cannabis.”
5. “Sustainable Development Goals.” SustainableDevelopment.UN.org. https://sustainabledevelopment.un.org/?menu=1300
6. Hazekamp, Arno. “The Trouble With CBD Oil.” Karger.com. June 2018. https://www.karger.com/Article/FullText/489287
7. Chandra, Suman, Lata, Hemant, ElSohly, Mahmoud. “Cannabis Sativa L. – Botony and Biotechnology.” Springer International Publishing. Edition 1. 2017.
8. “The Bioengineering of Cannabis.”
9. “The Bioengineering of Cannabis.”
10. Sismondo, Christine. “Flavonoids are the next Big Thing in Marijuana Research.” TheStar.com. July 23, 2019. https://www.thestar.com/life/health_wellness/2019/07/23/flavonoids-are-the-next-big-thing-in-marijuana-research.html
11. Charles, Shamard. “FDA, FTC Send Warning Letters to Three CBD Marketers for False Medical Claims.” NBCNews.com. April 2, 2019. https://www.nbcnews.com/health/health-news/fda-ftc-send-warning-letters-three-cbd-marketers-false-claims-n990251
12. “FDA requests data and information at public hearing on products containing cannabis or cannabis-derived compounds.” Lexology.com. May 31, 2019. https://www.lexology.com/library/detail.aspx?g=5344f064-5a68-40c5-8f69-ab5f90374b41
13. Ries, Julia. “CBD May Possibly Interfere with Your Daily Medication.” Huffpost.com. March 3, 2019. https://www.huffpost.com/entry/cbd-medication-interaction_l_5c9271efe4b08c4fec336ff2

14. Brown, JD, Winterstein, AG. “Potential Adverse Drug Events and Drug-Drug Interactions with Medical and Consumer Cannabidiol (CBD) Use.” NCBI.NLM.NIH.gov. July 8, 2019. https://www.ncbi.nlm.nih.gov/pubmed/31288397
15. “Cannabinoids 101: CBN.” Apothecarium.com. August 3, 2018. https://apothecarium.com/blog/nevada/2018/8/3/cannabinoids-101-cbn
16. Yar, Sanam. “What Is CBN? Cannabinol Is Said to Help with Sleep, But Here’s What Experts Have to Say About It.” Bustle.com. January 8, 2019. https://www.bustle.com/p/what-is-cbn-cannabinol-is-said-to-help-with-sleep-but-heres-what-experts-have-to-say-about-it-15726165
17. “Sleep and Sleep Disorder Statistics.” SleepAssociation.org. https://www.sleepassociation.org/about-sleep/sleep-statistics/
18. Lewis, Amanda Chicago. “Not Everybody Must Get Stoned: Pot’s Nonintoxicating Future.” WSJ.com. October 25, 2018. https://www.wsj.com/articles/prepare-for-a-wave-of-cannabis-productsbeyond-cbd-1540479300
19. “Cannabinoids 101: THCA.” Apothecarium.com. August 20, 2018. https://apothecarium.com/blog/nevada/2018/8/20/cannabinoids-101-thca
20. Rahn, Bailey. “What Is TCHA & What Are the Benefits of This Cannabinoid?” Leafly.com. March 17, 2015. https://www.leafly.com/news/cannabis-101/what-is-thca-and-what-are-the-benefits-of-this-cannabinoid
21. “Not Everybody Must Get Stoned: Pot’s Nonintoxicating Future.”
22. Havelka, Jacqueline. “What Is CBG (cannabigerol) & What Does This Cannabinoid Do?” Leafly.com. March 22, 2017. https://www.leafly.com/news/cannabis-101/what-is-cbg-cannabinoid

As Market for CBD Products Blooms, Questions Grow around Human Safety

1. Van Dolah, Harrison; Bauer, Brent A; Mauck, Karen F. “Clinicians’ Guide to Cannabidiol and Hemp Oils.” MayoClinicalProceedings.org. September 1, 2019. https://www.mayoclinicproceedings.org/article/S0025-6196(19)30007-2/fulltext
2. “From Farm to Aisle: 2019 U.S. CBD Market Report.” Brightfield.com. https://www.brightfieldgroup.com/library/us-cbd-market-report-2019
3. “CBD worth $22 billion by 2022? That’s crazy, right?” September 14, 2018. Brightfield.com https://www.brightfieldgroup.com/post/cbd-worth-22-billion-by-2022
4. “Licensed Hemp Acreage Quadruples Over 2018.” VoteHemp.org. September 5, 2019. https://www.votehemp.com/update/vote-hemp-releases-2019-u-s-hemp-grower-license-report-documenting-planned-hemp-cultivation-in-the-u-s/
5. U.S. Congress, House, Agricultural Improvement Act of 2018.HR 2, 115th Congress, 2nd Sess. https://www.congress.gov/115/bills/hr2/BILLS-115hr2enr.pdf
6. Hudak, John. “The Farm Bill, hemp legalization and the status of CBD: An explainer.” Brookings.edu. December 14, 2018. https://www.brookings.edu/blog/fixgov/2018/12/14/the-farm-bill-hemp-and-cbd-explainer/
7. U.S. Department of Agriculture. Executive Summary of New Hemp Authorities. May 28, 2019. Vaden, Stephen Alexander. https://www.ams.usda.gov/sites/default/files/HempExecSumandLegalOpinion.pdf
8. “FDA Regulation of Cannabis and Cannabis-Derived Products, Including Cannabidiol (CBD).” FDA.gov. November 13, 2019. https://www.fda.gov/news-events/public-health-focus/fda-regulation-cannabis-and-cannabis-derived-products-including-cannabidiol-cbd#food
9. “FDA Regulation of Cannabis and Cannabis-Derived Products, Including Cannabidiol (CBD).”
10. New Mexico Legislature. Enacting the Hemp Manufacturing Act. HB 581. July 1, 2019. https://www.nmlegis.gov/Sessions/19%20Regular/final/HB0581.pdf
11. U.S. Food and Drug Administration. “Warning Letter, Curaleaf, Inc.” July 22, 2019. https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/curaleaf-inc-579289-07222019
12. “What You Need to Know (And What We’re Working to Find Out) About Products Containing Cannabis or Cannabis-derived Compounds, Including CBD.” July 17, 2019. FDA.gov https://www.fda.gov/consumers/consumer-updates/what-you-need-know-and-what-were-working-find-out-about-products-containing-cannabis-or-cannabis
13. Hemp Production and the 2018 Farm Bill. Hearing before the United States Senate Agriculture, Nutrition and Forestry Committee. 116th Congress. (2019) (Testimony of Amy Abernethy) https://www.fda.gov/news-events/congressional-testimony/hemp-production-and-2018-farm-bill-07252019
14. Hemp. U.S. EPA Pesticide Program Dialogue Committee. May 8-9, 2019. https://www.epa.gov/sites/production/files/2019-05/documents/session-3-hemp.pdf
15. “Legal hemp raises questions about pesticides.” December 20, 2018. Purdue.edu. https://www.purdue.edu/newsroom/releases/2018/Q4/legal-hemp-raises-questions-about-pesticides.html

About Verisk

Verisk is a leading data analytics provider serving customers in insurance, energy and specialized markets, and financial services. Using advanced technologies to collect and analyze billions of records, Verisk draws on unique data assets and deep domain expertise to provide first-to-market innovations that are integrated into customer workflows. Verisk offers predictive analytics and decision support solutions to customers in rating, underwriting, claims, catastrophe and weather risk, global risk analytics, natural resources intelligence, economic forecasting, and many other fields. Around the world, Verisk helps customers protect people, property, and financial assets.

As highlighted throughout this report, we provide these solutions through various industry-leading brands, including ISO, AER, AIR, Geomni, Verisk Maplecroft, Verisk 3E, and Wood Mackenzie.