VERSPRITE

VerSprite Envisions 2019

Cybersecurity Through a Geopolitical Lens

Throughout 2018, businesses found themselves pawns in an environment of substantial geopolitical flux, with formerly stable areas suddenly undergoing changes that affect operating environments, reputations, and profitability. 2019 promises to be no less tumultuous, as a global economic slowdown, trade negotiations and trade wars, as well as high compliance costs and regulatory hurdles present major challenges for businesses in their primary markets, while the destructive consequences of climate change, challenges to inequality, and civil unrest affect progress in lucrative new markets.

- At the **global** level, corporate decision-makers must contend with leadership changes, evolving trade agreements or trade wars, and the effects of climate change, as the international economy begins to slow, and inequality rises. Nations not traditionally known for offensive cyber operations are likely to employ cyber attacks to boost their conventional means of power projection, and cyberattacks will begin to result in both direct and indirect deaths and injuries, while ransomware demands will shift from declining cryptocurrency to more valuable, and possibly non-monetary physical assets.

- At the **country** level, labor unrest, new regulatory regimes, and dependence on aging infrastructure vulnerable to debilitating ransomware attacks and cascade failure will require placating vocal workforces and finding workarounds to ensure business continuity.

- At the **local** level, a growing focus on moral hazards, and the evolution of the #MeToo movement will incentivize greater scrutiny and attempts to access data that can cast light on leaders rumored to be offenders, increasing financial costs (including settlements with accusers and ransom payments) while contributing to reputational harm.

Given the increases in vulnerability to geopolitical flux for companies of all sizes and in nearly every sector, due to the interconnectedness of supply chains, source codes, and payment platforms, every company needs to develop a **Corporate Geo-Cyber Strategy**, to ensure their business has a firm understanding of risk tolerance, exposure, and the requisite tools available to address emerging geopolitical risk and opportunities. As the only cybersecurity company with a geopolitical risk practice, VerSprite is ideally positioned to help each client develop and implement a highly customized Corporate Geo-Cyber Strategy through a range of advisory services and interactive simulations.

The inaugural edition, VerSprite Envisions 2019, is a general framework for identifying and understanding issues at the nexus of cybersecurity and geopolitical risk which are likely to affect most, if not all, businesses in the new year. Rather than seeking to predict the future, VerSprite Envisions seeks to identify the continuation or escalation of forces that will present both challenges and opportunities for businesses throughout the year, to serve as a starting point for companies developing and refining their Corporate Geo-Cyber Strategy. In-depth analyses for specific regions and sectors are available to VerSprite clients.

For more information, please contact **gpr@versprite.com**.

2019 Top Issues

at the Nexus of Cybersecurity and Geopolitical Risk

1. **Global Economic Slowdown**
2. **Politicized Technology: Forced Use or Banning of Technology Associated with State-Run Firms**
3. **Increased Technology Regulation and Rising Compliance Costs**
4. **EU Enforcement of Data Laws Begins in Earnest**
5. **Trade Wars, Trade Agreements, and Increasingly Weaponized Economic Interdependence**
6. **Tightening Belt and Uneven Road: China's Sweeping Initiative Hits Speed Bumps**
7. **Shifting Supply Chains and Blockchain Experimentation: The Risks of Haphazard Adoption**
8. **Cyber Threats and Infrastructure Vulnerability**
9. **Natural Disasters and Climate Change Consequences**
10. **Moral Hazard and #MeToo: Shifting Risk and Demanding Accountability**

Executive Summary

1

Issue Spotlight:

Global economic slowdown and bursting or shrinking bubbles will mean that 2018's roaring growth in much of the world will begin to slow given trade tensions, cryptocurrency value collapse, political crises, central bank activity, and increasing debt loads.

VERSPRITE VIEW: A global economic slowdown will force prioritization, affect pricing, hiring, and expansion. As companies seek robust insight into the geopolitical risks and opportunities presented by the changing economic environment, VerSprite can design and facilitate an interactive simulation to help a company analyze a difficult decision, or provide comprehensive vendor audits as companies seek to shift to lower cost alternatives or streamline operations.

2

Issue Spotlight:

Competition and strained relations between countries will result in businesses being required to use or to avoid certain technologies or platforms in order to be able to operate in foreign countries.

VERSPRITE VIEW: Greater focus on the geopolitical consequences of using certain hardware, firmware, and software will force companies to reevaluate enterprise tech decisions and seek alternatives to banned or compromised systems. VerSprite can provide assessments of alternative options and audit potential vendors to help companies determine the best enterprise tech solutions for their needs.

3

Issue Spotlight:

Increased data and privacy regulations will complicate business operations and raise compliance costs, while more sophisticated breaches and hacks will be larger and more damaging, as cybercriminals find ways to bypass previously strong measures like multi-factor authentication, and develop ways to fool biometric systems. Greater scrutiny of certain security protocols and their limitations will result in shifts to more invasive types of authentication. Advanced experimentation related to breakthroughs in fields such as gene editing will draw increased government attention and regulation.

VERSPRITE VIEW: To help companies better understand regulatory frameworks and compliance requirements, VerSprite provides comprehensive assessments, audits, and business continuity planning services, and can facilitate training simulations to help integrate new processes and protocols into employees' workflows to ensure compliance with new rules.

4

Issue Spotlight:

As the first wave of prosecutions and fines related to GDPR begin in earnest, firms will need to dedicate more money and effort toward compliance and training of employees. EU authorities will likely make examples of businesses who fail to comply with the data protections, including some small businesses that believe they can avoid scrutiny.

VERSPRITE VIEW: As companies face a landscape of increasing call for regulation, and plans in several countries to introduce legislation modeled on GDPR, VerSprite can prepare assessments detailing how pending legislation can affect company operations and what steps would be necessary to ensure compliance.

5

Issue Spotlight:

Trade wars, new trade agreements, and increased weaponization of economic interdependence to reward allies and punish adversaries will create complications for companies that have cross border operations in Europe, the Middle East, and Asia.

VERSPRITE VIEW: Tensions between the US and China will continue even if trade negotiations reach a positive outcome in late March and US companies with IP that China wants will face increased cyber attacks and attempts to steal that IP. As the only cybersecurity company with a geopolitical risk practice, VerSprite can provide companies with services to better understand their geopolitical exposure and take steps to ramp up cybersecurity measures.

6

Issue Spotlight:

The Belt and Road Initiative (BRI) will suffer from delays, incomplete projects, and reevaluations of agreements in response to protests about unfair deal terms, lack of promised new jobs for locals, continued importation of Chinese laborers, and unacceptable levels of debt.

VERSPRITE VIEW: As China faces greater backlash and delays in BRI projects, there are opportunities for companies from other countries to take advantage of gaps to step in and provide services under better terms. To better inform decision-makers considering such steps, VerSprite provides robust market entry assessments and cyber-geopolitical risk exposure assessments.

7

Issue Spotlight:

Attempts to use blockchain to secure supply chains and cut down on waste/fraud are likely to fail to address root causes of these issues. Uneven application of blockchain technologies for industries in which the distributed ledgers are poorly matched to the factors driving waste and fraud are instead likely to exacerbate those problems.

VERSPRITE VIEW: Through supply chain security assessments, VerSprite can provide decision-makers with insight to help understand whether blockchain and other developments would help mitigate threats to supply chain security, and help companies understand geopolitical threats to their supply chains.

8

Issue Spotlight:

2019 will likely have the first directly attributable deaths as a result of cyberattacks on sensitive infrastructure, like hospitals, power grids, and transport hubs.

VERSPRITE VIEW: VerSprite's Virtual Geopolitical Risk Officer service, in tandem with a suite of remediation services, can help companies integrate ongoing monitoring to help quickly identify breaches or more effectively recover from such attacks. Firms who operate or depend heavily upon sensitive infrastructure need risk identification and mitigation to be conducted not on a compliance- driven basis but continuously, with simultaneous attention properly placed on internal cybersecurity defenses and the external geopolitical threat landscape.

9

Issue Spotlight:

More frequent and more damaging natural disasters, as well as the consequences of climate change in places that have limited food and water stores will continue throughout 2019. Delayed rebuilding of areas devastated in hurricanes in 2017 show the extent to which even advanced countries struggle with the cost and resources needed to rebuild, resulting in uneven progress. As countries try to address climate change, and shift away from traditional sources of power, like coal, there will be opportunities to invest in modern and more sustainable infrastructure projects.

VERSPRITE VIEW: As companies work to mitigate the effects of climate change on their operations and supply chains, or take advantage of new opportunities presented by new shipping routes and technological advancements, VerSprite simulations can offer companies a way to explore these decisions via interactive tabletop exercises that include insight from all teams within the organization, and contend with the possible consequences of various decisions.

10

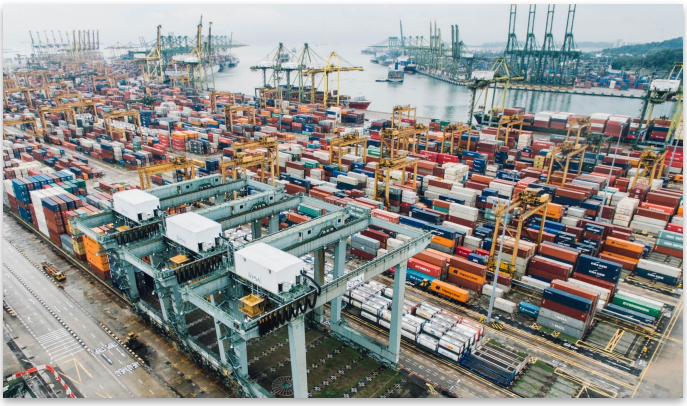
Issue Spotlight:

Moral hazard (aggressive risk-taking given limited consequences for the risk taker) will continue to be a major driver of crises in 2019. But even as some are incentivized to take risks while protected from the ramifications of failure, others will be incentivized to demand accountability as the #MeToo campaign evolves, and initial measures taken to address or head off #MeToo allegations will themselves cause problems.

VERSPRITE VIEW: VerSprite provides in-depth due diligence assessments to help companies assess potential new hires, acquisitions, and partners to uncover any potential problems that could yield reputational or legal issues.

Global economic slowdown and bursting or shrinking bubbles will mean that 2018's roaring growth in much of the world will begin to slow given trade tensions, cryptocurrency value collapse, political crises, central bank activity, and increasing debt loads.

Macro – As the cryptocurrency and technology startup bubbles pop, real estate and entertainment markets are likely to feel the squeeze. Estimates for global growth in 2019 have fallen from 3.9 percent to 3.7 percent, per **International Monetary Fund** projections. Highly valued tech startups are beginning to shut down in several parts of the world, including the US, UK, and beyond, as astronomical valuations are undermined by slow or nonexistent progress, as well as legal troubles.



As Brexit remains unsettled, companies find themselves forced to delay plans or gamble on shifting locations to the continent to benefit from remaining within the EU, without fully understanding what the UK relationship with the EU will be after March 29, 2019. Pressure to cut costs may drive some companies to seek less costly cybersecurity solutions, endangering intellectual property and sensitive data. As economies sputter, crime, including AI-based cybercrime and more nefarious uses of malicious botnets via quickly proliferating unsecured IoT devices, will increase.

Strategic – Currency fluctuations will affect pricing models, requiring greater emphasis on ensuring that products are correctly priced for specific market conditions. Funding may not be as abundant in tighter markets, as access to cheap debt dries up. Investor decisions to wait out a period of uncertainty and currency fluctuation may delay some projects.

Rising pressure to secure good deals on M&A may delay such processes, increasing the likelihood that a leak or cybersecurity breach may endanger a potential deal or serve as an excuse to drive an acquisition price down.

Operational – Delayed or reduced hiring, tighter budgets, and fewer resources may affect vendor procurement, resulting in insufficient due diligence, or shifts to cheaper (but lower-skilled) labor in markets substantially affected by trade tensions. Companies will be pressured to allow employees to move out of expensive cities to lower cost alternative locations, creating more distributed workforces and increasing potential vulnerabilities from distributed systems and hardware. Government hiring in countries facing economic pressure may slow down, so bureaucratic processes associated with business operations will have an even slower turnaround time.

Micro – As real estate markets shift, and consumers look to cut costs in an environment of uncertainty, cities will have to work harder to create more favorable conditions to incentivize business creation. There will be increased competition to bring major company hubs to struggling cities, driving cities into debt as they try to provide the most attractive portfolio of incentives.

VerSprite View

A global economic slowdown will force prioritization, affect pricing, hiring, and expansion. As companies seek robust insight into the geopolitical risks and opportunities presented by the changing economic environment, VerSprite can design and facilitate an interactive simulation to help a company analyze a difficult decision, or provide comprehensive vendor audits as companies seek to shift to lower cost alternatives or streamline operations.

Sources: *IMF cuts world economic growth forecasts on tariff war, emerging market strains*

Competition and strained relations between countries will result in businesses being required to use or to avoid certain technologies or platforms in order to be able to operate in foreign countries.

Macro – More companies will be required to use a certain platform in partnerships with a foreign partner or client (for example, companies in China may require the use of Huawei products and platforms).

Companies engaged in projects outside their home countries may find themselves forced to find workarounds for platforms that are banned or blacklisted in those countries (for example, Britain's BT Group banned the use of Huawei equipment for their 5G rollout and is phasing it out of its core networks). Intellectual property theft will escalate, as countries battle for edge in a slowing global economy.

Strategic – Decision-makers will require a better understanding around questions such as which platforms are indispensable, which can be replaced or adapted, and what reputation costs they face for using a platform or hardware blacklisted in some countries.

If a requirement cannot be negotiated, they will have to consider additional costs related to securing compromised or lower quality platforms. Comprehensive strategies to combat IP theft will dramatically increase cybersecurity spending.

Operational – At the operational level, companies will need to allocate additional resources devoted to comprehensive due diligence on potential platforms or technology, additional resources deployed to address increased vulnerability and exposure, and ongoing monitoring to ensure systems and data are well protected, particularly with regards to increasingly growing populations of remote workers using their own devices for work.

It is **projected** that remote workers will constitute a third of the workforce within 10 years. Leadership will face further protests from employees about certain contracts supporting government agencies.

Micro – On a day to day basis, possible solutions include robust and effective training for employees, practical workarounds, and shifting some responsibilities to certain countries where the environment is more favorable. Workforces may protest being forced to use platforms known to be compromised by government backdoors, or leak information regarding breaches that leadership tries to cover up. Countries that are hard hit by bans on state company technology will seek to quietly buy or invest in similar companies in those countries, to retain some access.

VerSprite View

Greater focus on the geopolitical consequences of using certain hardware, firmware, and software will force companies to reevaluate enterprise tech decisions and seek alternatives to banned or compromised systems. VerSprite can provide assessments of alternative options and audit potential vendors to help companies determine the best enterprise tech solutions.

Source: *Future Workforce Report*

Increased data and privacy regulations will complicate business operations and raise compliance costs, while more sophisticated breaches and hacks will be larger and more damaging, as cybercriminals find ways to bypass previously strong measures like multi-factor authentication, and develop ways to fool biometric systems.

Greater scrutiny of certain security protocols and their limitations will result in shifts to more invasive types of authentication. Advanced experimentation related to breakthroughs in fields such as gene editing will draw increased government attention and regulation.

Macro – Regulation of data and user privacy will continue in 2019, requiring that companies understand, adhere to, and find ways to reconcile competing regulations and costly compliance requirements. In preparation for GDPR, companies spent between $1 million and $10 million each to ensure compliance, per a PWC **survey**. Already, more than 80 countries **regulate** data, and dozens more are considering legislation, increasing the burden on companies that tend to operate in dozens of countries and will be forced to comply with dozens of sometimes competing regulations.
On average, data law compliance costs a firm about $5.5 million annually, a 43 percent increase from 2011, according to a **Ponemon Research Institute** study. Biometric identity programs will proliferate widely, but insufficient prioritization of security will lead to lawsuits seeking to stop such programs for the tracking of residents. Innovation in biotech and fintech is likely to find more opposition, even in China, where CRISPR and other initiatives face comparatively lower hurdles. Testing bans on animals and humans will proliferate and medical testing rules will intensify.

Strategic – Tighter rules will raise compliance costs and result in losses in industries like agriculture, where profit margins are already tight. As countries seek advantage in a tight environment, they will focus on spurring domestic agriculture and production capabilities, making them harder to leverage.

Uneven success in this mission will lead to halted and redesigned policies, contributing to flux in these sectors throughout 2019.

Operational – Though a focus on developing domestic sectors will bring increased funding to such initiatives, long term viability will be uncertain for countries that lack the skilled labor, and other necessary inputs. Companies will dedicate greater funding to identifying and finding workarounds, as well as accelerating domestic development of necessary resources.

Micro – Companies that have built their businesses on pervasive but targeted platforms will go out of business, particularly in emerging markets. Vendors and third parties who currently use a banned technology or product, or which fail to abide by demands to use or refrain from using certain technology, will be forced to transition or risk going out of business.

Companies that fail to properly secure and control entry to their services, or do not increase security measures for storing sensitive information and user data, will be called out and possibly penalized.

VerSprite View

To help companies better understand regulatory frameworks and compliance requirements, VerSprite provides comprehensive assessments, audits, and business continuity planning services, and can facilitate training simulations to help integrate new processes and protocols into employees' workflows to ensure compliance with new rules.

Sources: *Pulse Survey: GDPR budgets top $10 million for 40% of surveyed companies*
Data Protection Around the World, *The True Cost of Compliance with Data Protection Regulations*

As the first wave of prosecutions and fines related to GDPR begin in earnest, firms will need to dedicate more money and effort toward compliance and training of employees. EU authorities will likely make examples of businesses who fail to comply with the data protections, including some small businesses that believe they can avoid scruting.

Macro –As the first wave of prosecutions under GDPR continues in 2019, representing the first real tests of the sweeping data protections, other countries will consider the benefits and costs of imposing similar regulatory regimes.

Some countries will seek to constrain foreign companies while protecting and enhancing the environment for domestic firms. Companies counting on fines being an acceptable cost of continuing to do business may find themselves targeted under further rules to discourage GDPR violations or raise the risks of failing to comply.

As terrorist attacks continue in Europe, law enforcement agencies will require greater cooperation and information sharing, leading to increasing requests for data and demands that terror-related content be removed from online platforms.

Strategic – Additional announcements of data breaches will drive higher numbers of people to abandon certain platforms which are deemed insincere in promises to safeguard information and user privacy.

GDPR will do little to cut down on spam and cybercrime, as cybercriminals will continue to benefit from the wealth of data revealed in past breaches and find creative ways to further increase their efforts.

Operational – Areas that have looser regulations will see an increase in investment, though the boost will be short-lived as other countries crack down on attempted workarounds or attempts to creatively bypass the spirit or intent of laws protecting data and privacy.

Companies will need to have workflows in place to identify any content for which they could be fined, and ensure that such processes are aligned with deadlines for content removal or data sharing.

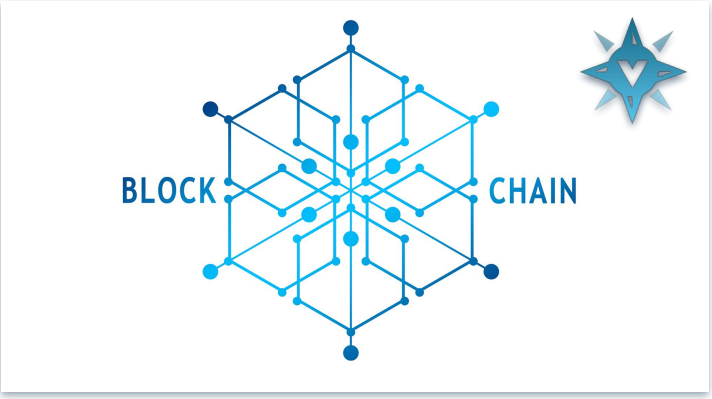
Micro – Given the high possible penalties associated with non-compliance or violation of GDPR, some of the businesses hit by major fines will be forced to close, and examples are likely to be made of smaller companies that believe they can bypass compliance without consequences. In the wake of the first GDPR prosecutions, businesses will have to intensify and expand employee training and ensure daily workflows comply with regulations.

VerSprite View

As companies face a landscape of increasing call for regulation, and plans in several countries to introduce legislation modeled on GDPR, VerSprite can prepare assessments detailing how pending legislation can affect company operations and what steps would be necessary to ensure compliance.

Source: *The EU General Data Protection Regulation*
Germany's first fine under the GDPR offers enforcement insights

Trade wars, new trade agreements, and increased weaponization of economic interdependence to reward allies and punish adversaries will create complications for companies that have cross border operations in Europe, the Middle East, and Asia.



Macro – Ongoing tensions between China and the US are likely to escalate and manifest in ways that require businesses to find alternate supply chain routes, suppliers, and sources of natural materials, forcing some businesses to shift production and supply chains to more expensive locations.

This will in turn raise prices on some goods and may affect consumer sentiment. Ripple effects from the trade war are likely to affect businesses in the first half of 2019 even if talks between China and the US are successful in reaching an agreement. The fate of the US-Mexico-Canada Agreement (USMCA) intended to replace NAFTA, is unclear following a new Democratic majority in the US House of Representatives, and a new presidential administration in Mexico.

Ongoing uncertainty over Brexit will stretch into 2019, even as the deadline for making a deal approaches, presenting a challenge to companies awaiting clarity on the terms of the deal before making major decisions. The auto industry is likely to be hardest hit by trade wars, new agreements, and a global economic slowdown.

Strategic – As companies adjust to an era of greater competition between China and the US, and new trade agreements governing relationships between near neighbors, and the UK with Europe, risk arbitrage will be a main focus of decision-makers considering major investments and joint partnerships with allies of both powers.

To take advantage of more favorable conditions, or insulate themselves from the consequences of eroding relations, companies will have to spin off separate entities, and add layers or separation to their operations, both of which increase costs and complexity.

Operational – Tensions will lead to suspended joint projects and close working relations, delaying progress, and resulting in lost funding for some endeavors. Promised benefits – lower tariffs and higher wages for union workers - will be delayed as the agreement remains unratified. Companies that rely on favorable NAFTA measures to stay in business will feel the pressure to ramp up and secure sales of major items, including cars for example, before prices are expected to rise under USMCA terms.

Micro – Smaller companies reliant on previously good relations between China and US may go out of business as both governments seek to target the other's companies through tariffs, and other economic instruments, including increased regulatory scrutiny. Larger firms invest more heavily in domestic capabilities to avoid paying high tariffs, but thereby either risk reducing profits or pass the cost on to consumers. Strained relations will affect everything from hiring decisions to what technology businesses will use on a daily basis.

VerSprite View

Tensions between the US and China will continue even if trade negotiations reach a positive outcome in late March and US companies with IP that China wants will face increased cyber attacks and attempts to steal that IP. As the only cybersecurity company with a geopolitical risk practice, VerSprite can provide companies with services to better understand their geopolitical exposure and take steps to ramp up cybersecurity measures.

Sources: *Auto industry caught in the trade war crosshairs*, *US-China Business Council 2018 Member Survey*

The Belt and Road Initiative (BRI) will suffer from delays, incomplete projects, and reevaluations of agreements in response to protests about unfair deal terms, lack of promised new jobs for locals, continued importation of Chinese laborers, and unacceptable levels of debt.

Macro – Despite much fanfare and sweeping pronouncements, many projects announced as part of the Belt and Road Initiative, spread over nearly 100 countries and estimated to be worth more close to $1 trillion, will remain untouched throughout 2019, and projects in progress may be hit by delays as populations protest deal terms that are considered unfair or contribute to an unacceptably high sovereign debt burden.

Already, projects worth $22 billion in Malaysia have been cancelled over political concerns, and several other countries are pausing to review the terms of deals. Uneven progress will delay anticipated supply chain streamlining, and force some countries to postpone major infrastructure projects.

Strategic – Leaders may be challenged by opposition politicians for any deals made with China that are likely to bind countries to unfair terms, potentially unseating leaders perceived to enjoy widespread support. Allegations of fraud and corruption are likely to increase, creating a boon for the legal industry.

Operational – Due to a greater focus on the details of the terms of Belt and Road deals, areas with controversial projects will experience increased scrutiny of the exact terms, and investigations of any allegations of fraud or corruption are likely to be taken seriously in places with robust and independent media and judiciaries. In places without opposition, rushed or poor quality projects will contribute to disruptions in industries like air travel, port security, and power infrastructure.

Micro – Underserved areas relying on new infrastructure to be built as part of the Belt and Road Initiative are unlikely to see even progress, and companies participating in the initiatives may find themselves side-lined as Chinese-led projects continue to shift away from promised use of local labor to dependence on Chinese laborers brought in to handle construction.

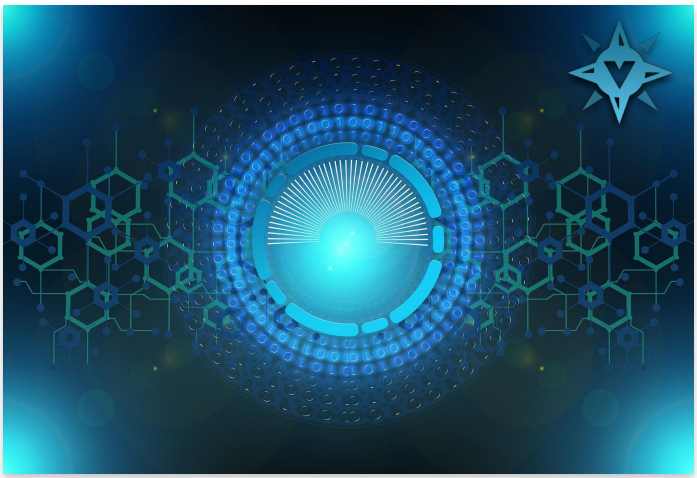
This will lead to greater labor and civil unrest, and possible violence or property destruction, in places where promised jobs do not materialize.

VerSprite View

As China faces greater backlash and delays in BRI projects, there are opportunities for companies from other countries to take advantage of gaps to step in and provide services under better terms. To better inform decision-makers considering such steps, VerSprite provides robust market entry assessments and cyber-geopolitical risk exposure assessments.

Source: *China's Silk Road isn't so smooth*
Chinese private investment in belt and road projects may be losing steam

Attempts to use blockchain to secure supply chains and cut down on waste/fraud are likely to fail to address root causes of these issues. Uneven application of blockchain technologies for industries in which the distributed ledgers are poorly matched to the factors driving waste and fraud are instead likely to exacerbate those problems.



Macro – Despite estimates that blockchain technology could save the logistics industry hundreds of billions of dollars (and IBM predictions that ocean shipping alone could shed **$38 billion** annually in costs), the technology has not been broadly adopted because of its many drawbacks, including the slow pace of transactions, the increased costs of running multiple nodes, and repeated forks, as well as major hacks.

Attempts to secure supply chains, such as food moving from farm or factory to table, or diamonds from mine to store using emerging technologies like blockchain, will fail to address core issues.

Food safety rules will be tightened in the wake of several deadly contaminated food cases but attempts to rely on technology without addressing problems like water regulations and waste removal will mean more such cases, not fewer, as blockchains merely create an illusion of safety.

Strategic – Companies will need to carefully assess the pros and cons of transitioning to blockchain-based processes, requiring investment in studying the technology's applicability, benefits, and vulnerabilities.

Inadequate assessments or dismissal of major issues with blockchain will result in losses or complications for companies that pursue blockchain integration without adequate insight or incomplete information, as these companies become attractive attack targets.

Operational – Smart contracts, one of blockchain's main features, will be particularly attractive to many businesses, including small and medium sized enterprises.

However, vulnerability to hacks, and the exorbitant costs of recovering from a hack, will delay the technology's large-scale implementation. In just the first three quarters of 2018, hacks netted cybercriminals **$1 billion**.

Micro – As businesses attempt to integrate blockchain into daily workflows, in an effort to use the distributed ledger technology to reduce barriers to new markets and insulate themselves against risks, newly discovered flaws in the much hyped - but not nearly immutable - technology will lead to daily disruptions and delays, necessitate redundancies, and drive up the very costs and delays blockchain is meant to eliminate.

VerSprite View

Through supply chain security assessments, VerSprite can provide decision-makers with insight to help understand whether blockchain and other developments would help mitigate threats to supply chain security, and help companies understand geopolitical threats to their supply chains.

Sources: *Maersk and IBM are bringing blockchain tech to the shipping industry*
Cryptocurrency Anti-Money Laundering Report

2019 will likely have the first directly attributable deaths as a result of cyberattacks on sensitive infrastructure, like hospitals, power grids, and transport hubs.

Macro – 2018 saw an increase in the number of ransomware attacks against state governments and hospitals, rendering government officials and medical staff incapable of fulfilling their duties, and delaying ambulance, operations, and other critical elements. States and hospitals paid out millions in ransoms - with Atlanta's city government spending as much as **$17 million** to recover from a major attack. Such payouts affect budgets for other services and exposing the lack of adequate cyber security and protections for essential entities.

Given the extent to which these attacks exposed glaring vulnerabilities, and the length of time required to remediate these issues, increased attacks will take place throughout 2019 as businesses try to catch up and protect themselves. An attack during a natural disaster would be particularly devastating.

With the sharp declines in bitcoin and other cryptocurrency values, cyber-physical ransomware will be a risk to businesses in 2019, as cybercriminals shift away from demanding cryptocurrency ransoms and set their sights on higher value assets. Thieves will target infrastructure, cutting people off from cellular service and power in rural areas, affecting those people's ability to call for help when needed.

Strategic – Businesses seeking cybersecurity insurance against ransomware threats will find themselves paying extremely high premiums or investing high sums in advanced security measures, though low-tech penetrations will still succeed in hobbling some entities. Insurance companies that extend policies to businesses that do not adequately remediate vulnerabilities may be devastated by payouts. Major cities will seek to insure themselves against such events, presenting an opportunity for the insurance industry.

Operational – Companies will struggle to fill openings for cybersecurity positions, resulting in weaknesses in their ability to deploy cybersecurity measures, and will need to increase salaries to attract limited numbers of available skilled workers. Lack of qualified candidates will make proffered technology solutions more attractive to companies that cannot find the right employees, but over reliance on technology will itself increase vulnerability to breaches and attacks.

Micro – Enhanced cybersecurity measures will slow daily workflows and affect productivity if implemented incorrectly. Businesses that fail to take the threat seriously will find themselves unable to operate if targeted by ransomware demands that exceed available funds. Lawsuits may devastate even those who manage to pay the ransom, if injuries or deaths occur while the facility is incapacitated and incapable of fulfilling its responsibilities.

VerSprite View

VerSprite's Virtual Geopolitical Risk Officer service, in tandem with a suite of remediation services, can help companies integrate ongoing monitoring to help quickly identify breaches or more effectively recover from such attacks. Firms who operate or depend heavily upon sensitive infrastructure need risk identification and mitigation to be conducted not on a compliance-driven basis but continuously, with simultaneous attention properly placed on internal cybersecurity defenses and the external geopolitical threat landscape.

Source: *CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million*

More frequent and more damaging natural disasters, as well as the consequences of climate change in places that have limited food and water stores will continue throughout 2019. Delayed rebuilding of areas devastated in hurricanes in 2017 show the extent to which even advanced countries struggle with the cost and resources needed to rebuild, resulting in uneven progress. As countries try to address climate change, and shift away from traditional sources of power, like coal, there will be opportunities to invest in modern and more sustainable infrastructure projects.

Macro – More devastating natural disasters, including earthquakes, hurricanes, tsunamis, and droughts will take place in 2019, particularly in parts of Africa, the Middle East, and the Caribbean. Companies building new locations will need to consider the effects that such natural disasters and climate change could have on their facilities. Internet connectivity, electricity, and other communications infrastructure damage may reduce productivity and affect GDPs of economies where prolonged reconstruction periods delay rebuilding.

Disaster recovery firms will have no shortage of opportunities but will need to invest in insight to protect their operations in affected areas. **September** is traditionally the costliest month of each year, as global tropical cyclone activity is highest, and it was no exception in 2018, when several hurricanes, typhoons, tsunamis, and earthquakes caused tens of billions of dollars in damage in dozens of countries.

The Camp Fire, the largest in California's history, is estimated to have done **$9 billion** in damage in November 2018.

Strategic – Companies that rely primarily on tourism to areas prone to natural disasters or already experiencing the effects of climate change will have to expand their focus to areas that are more insulated from the effects of such events. As countries face the likelihood of devastating events, they will force companies to conduct more comprehensive due diligence, which will raise the costs of compliance with more in-depth studies of viability, environmental impact, and site restoration.

The insurance industry will reevaluate offerings as natural disasters shed light on underinsured assets, as businesses work to reduce gaps in coverage and seek to protect themselves from uninsured losses, particularly in emerging markets. As much as **$163 billion** worth of global assets in emerging markets are estimated to be uninsured, per Lloyd's of London.

Operational – As countries try to address pollution, overuse, and human damage to certain areas, more closures of popular beaches/islands/destinations, or limitations on the number of visitors, may present substantial challenges to business continuity for companies in the hospitality and tourism sectors, with downstream effects for their vendors.

Micro – Businesses located in areas already seeing the effects of climate change will have to explore alternative locations or invest in measures to prevent their facilities from being overwhelmed by natural disasters or changing climates, including the construction of hardened structures, retrofitting of buildings that cannot withstand certain events, and other remediation efforts.

VerSprite View

As companies work to mitigate the effects of climate change on their operations and supply chains, or take advantage of new opportunities presented by new shipping routes and technological advancements, VerSprite simulations can offer companies a way to explore these decisions via interactive tabletop exercises that include insight from all teams within the organization, and contend with the possible consequences of various decisions.

Sources: *Global Catastrophe Recap- September 2018*, *RMS Estimates Insured Losses, From The Camp and Woolsey Wildfires To Be Between USD $9 Billion and $13 Billion*, *Emerging economies have $160bn insurance gap*

Moral hazard (aggressive risk-taking given limited consequences for the risk taker) will continue to be a major driver of crises in 2019. But even as some are incentivized to take risks while protected from the ramifications of failure, others will be incentivized to demand accountability as the #MeToo campaign evolves, and initial measures taken to address or head off #MeToo allegations will themselves cause problems.

Macro – Throughout 2018, there were several breaking news stories alleging stunning accusations - such as Bloomberg's investigation of alleged Chinese infiltration of hardware manufacturers Supermicro using tiny chips. Companies targeted in such allegations suffered reputational damage and stock price drops, and other consequences, despite a lack of evidence to support the allegations. Those who wrote the pieces suffered little for making what appear to be unfounded claims, making it likely that other companies who find themselves in positions of geopolitical significance may be targeted in similar situations. On the flip side, the ongoing campaign to demand accountability of powerful individuals accused of sexual harassment and abuse will extend into 2019, after more than **425 high ranking people** were accused of related crimes in 2018.

#MeToo allegations will expand to sectors beyond government, media and entertainment. Men in power who seek to avoid any situations that could lead to or be interpreted as inappropriate behavior may seek to avoid hiring women as assistants or deputies, making them targets of accusations that they are then impeding diversity efforts.

Strategic – Firms that build sensitive hardware or provide services to powerful global companies may find themselves targeted by allegations of tampering, espionage, and other misdeeds, requiring constant self-assessment of vulnerabilities and exposure to larger conflicts within which they may become involved. Sustained campaigns to uncover evidence of wrongdoing will incentivize cybercriminals hoping to obtain high levels of compensation for hacking influential companies to uncover compromised supply chains or evidence of misdeeds.

Operational – Governments and boards will seek to disincentivize excessive moral hazard by removing loopholes around accountability.

Businesses will need to demonstrate progress in hiring and promoting female candidates, ensuring equal treatment and pay, and supporting broader initiatives at the highest levels of the company.

Businesses will need to perform careful diligence on NGOs and organizations with which they partner to promote such practices.

Micro – There will be higher demand for companies to have "skin in the game" to borrow Nassim Taleb's term, as the opposite of moral hazard. On the #MeToo front, greater scrutiny of hiring practices and statistics with regard to women candidates, equal pay, and diversity, and lawsuits will increase against those companies thought to be gaming the system.

In an effort to protect company confidential information, employees may face additional security measures that slow productivity as companies try to boost cyber and physical security protections to prevent themselves from being targeted by hacktivists and others looking for evidence of wrongdoing.

VerSprite View

VerSprite provides in-depth due diligence assessments to help companies assess potential new hires, acquisitions, and partners to uncover any potential problems that could yield reputational or legal issues.

Source: *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*
#MeToo: One Year Later

VerSprite Geopolitical Risk Service Suite

VerSprite Geopolitical Risk helps formulate a holistic approach toward clients' overall risk landscape, advising on global threats and opportunities, analyzing business impact from political, socioeconomic and cultural trends, especially as drivers of information security issues. As businesses confront their growing exposure to the interrelated issues at the nexus of cybersecurity and geopolitical risk described in this overview, and the effect it can have on their reputations, operations, and prospects for growth in markets abroad, it's vital they have a trusted partner to help them assess and remediate their exposure, analyze decisions, and simulate the consequences of likely future scenarios.

ADVISORY SERVICES

VerSprite Geo-Cyber advisory services provide clients with highly customized and comprehensive findings presented in a report and delivered in an interactive briefing. Analysis is based on the scope and positioning of global presence, including physical and human assets, corporate cyber footprint, and other dependencies around domestic and foreign socioeconomic and political forces.

- Geo-Cyber Exposure
- Market Entry
- M&A/Joint Partnership Due Diligence
- Supply Chain Risk
- On-Demand Consultation Session

INTERACTIVE SIMULATION EXPERIENCES

VerSprite designs and facilitates tabletop exercises that serve to stress-test your organization on mitigation strategies and assess your ability to address threats stemming from geopolitical causal factors, as well as analyze complex questions, and train teams to follow more effective practices. To learn more, contact us today at **gpr@versprite.com**.