Teneo

Vision

Edition 5 | 2018

Where Is The World Going? How Do We Get There First?

Editor | James Hoge

Risk in the World

Be Aware, Not Afraid

William J. Bratton, Executive Chairman, Teneo Risk

When it comes to crisis, it's not "if," it's "when." That is the one certainty that emerges from the uncertainty around us as we anticipate, mitigate, and navigate non-economic risk. Thus, while granular predictions of what will happen in 2018 are not possible, I can share these expectations: terror and the methods of its execution will increase; civil disorder will further strain our polity; fresh international perils will join familiar ones; new diseases will test preparedness; America will continue to shift the ways it engages with the world; and cyber security threats will consume more and more corporate resources. As these assumptions indicate, risk and uncertainty are intertwined, and both can occasion fear. However, awareness trumps fear, and preparation can turn risk into opportunity.

When assessing these and other vulnerabilities, leaders must think in terms of strategic goals. Strategic thinking means seeing around corners. Corporate leaders must also be constantly aware that potential crises involve the safety of people, and a company is nothing without its people.

Terror's Shifting Profile

In the sixteen years since September 11th, terrorism has shifted, morphing from grandiose sophistication to simple, terrible functionality — from four simultaneously-hijacked jetliners destroying buildings and military installations to a rented Renault plowing through crowds on a promenade. Throughout the period, terrorist actors have functioned within one of three buckets: inspired, enabled, or directed. Over the past five years, however, the distribution has changed.

'Inspired' is synonymous with an actor or actors, working alone or in tight, frequently familial groups, who have no direct contact with the leaders or agents of the terrorist organization they support. These are often called 'lone wolf' attacks. The attack in San Bernardino, in December 2015, is an example.

'Enabled' is synonymous with an actor or actors who have been in direct contact with and are encouraged or guided by the terrorist organization. The Fort Hood shooting in November 2009 fits this category.

Finally, there is 'directed.' This is synonymous with an actor or actors who have been trained, and/or equipped, and/or deployed by handlers or leaders in the terrorist organization. The September 11th attacks are the exemplar of this. The Mumbai attacks in November 2008 and the Paris attacks in November 2015 are additional examples.

During the first decade of the 21st Century, most plots were 'directed.' Terrorists, acting alone or in cells, were in contact with leaders or their agents. The bad news was that these plots, when they worked, were devastating, with high body counts and high publicity. The glimmer of good news, only appreciated in retrospect, was that they were relatively infrequent and could be disrupted.

Since 2014, however, the rise of Abu Bakr al-Baghdadi and ISIS in Syria — and their ability to leverage social media to inspire or enable malefactors who could never be effective in a directed operation — has diverted an increasing number of acts into the first two buckets. ISIS didn't invent propaganda; Al Qaeda first issued *Inspire*, the online magazine that helped motivate the Boston Marathon bombers, in 2010. However, ISIS improved the model, using Twitter and high-production video and encrypted communications tools. Their own online magazine, *Dabiq*, which debuted in 2014, has been a tremendously effective recruitment tool, helping the ISIS model to metastasize.

The ISIS narrative of 'bombs, bullets, cars, and fire' has meant many more attacks. It has allowed anyone who hates the West, seeks empowerment and belonging, and loves a warped vision of Islam, to grab whatever's at hand — gun, hatchet, knife, car keys — to become a jihadi. No training, no complicated bombmaking, no arduous trip to the Pakistani frontier or the Levant. Such attacks are generally smaller in scope, with fewer deaths, but they are easier to execute. They are also harder to disrupt. Someone reading *Dabiq* on the dark web and stewing in his own hate cannot be discovered by signals intelligence or by capturing and interrogating an al Qaeda handler in Idlib (a governate region in Syria mostly controlled by the Al-Nusrah Front, an al Qaeda offshoot).

This means that the pace of attacks, which has accelerated since 2015, will not diminish in 2018. ISIS has experienced setbacks – the diminishing caliphate in Syria, the possible death of al-Baghdadi – but they are setbacks that may actually aggravate the problem. Trained fighters will likely be among those fleeing the region; adherents who never fought but observed from afar will have new injustices to avenge. Worse, ISIS methods are being adopted by other groups; indeed, the vehicular assault by a white supremacist in Charlottesville serves as one example of this. Al Qaeda, for its part, is forging alliances throughout the Maghreb and the Horn of Africa. In corporate terms, ISIS represents a new economy, expanding its network by activating malefactors via earned media contacts, while blue chip al Qaeda works M&A with existing networks. The older group isn't ignorant of branding, however. In 2018 you can expect Osama bin Laden's son, Hamza, to seek to establish a higher profile.

Law enforcement has attempted to adjust to this. I led the New York Police Department (NYPD) through a reevaluation and reorientation of its counterterrorism efforts, ensuring we had the capacity to respond to the types of attacks that ISIS had normalized, even as we continued to be ready for the larger events that Al Qaeda favored (and which ISIS conducts as well). We anticipated – and moved to mitigate – so that when an attack strikes, the NYPD will be well prepared to navigate the situation in whatever form it takes. Municipalities and companies need to follow suit. Owing to new trends in low-tech vehicle-based attacks, they can start with bollards (posts installed to control road traffic and designed to prevent car-ramming attacks) and vehicular-access controls. Had such structures been in place in Barcelona this past August, fewer people might have been killed.

Civil Disorder

I fought in Vietnam and saw the protests when I came home. I was a cop in Boston, and policed the clashes over bussing. I've dealt with disorder and demonstrations for nearly fifty years. None were as fraught as the anti-police marches in New York City in late 2014 and early 2015. But what comes next may be worse; hate has emerged from out of the shadows.

It will not go back easily. The Southern Poverty Law Center tracks more than 900 American hate groups. In Charlottesville, Virginia, we saw hate emboldened, without masks or hoods; we saw its provocations and violence. All of us should recoil from Nazism and white supremacy and oppose hate — but some of that opposition will spill into civil disorder. In 2018, I anticipate it will be particularly pronounced on college campuses. (From Vietnam, to Apartheid, to the Occupy movement, the passion to tackle injustice as one sees it is part and parcel of a being a student.)

This heightened potential for disorder is exacerbated by the fact that extremist groups, whether alt right or the black bloc elements of the Antifa, have expanded their respective modus operandi this year, often by adopting their adversaries' tactics. In New York City, alt right protestors interrupted Shakespeare in the Park using methods associated more frequently with the left; an active shooter, who was apparently motivated by leftist politics, attacked the Republican congressional softball team in Virginia; a neo-Nazi, using an ISIS-style vehicle attack, killed and injured anti-white supremacist protestors in Charlottesville.

As the risk of disorder grows, municipalities must confront the fact that, although police have the tools to quell riots, few departments have the training to prevent them. Policing needs equipment like riot gear and tactics like skirmish lines, but misapplication of those tools can sometimes tip unrest into riot. Instead, police departments need to navigate, mitigate, and anticipate - focusing on synchronized movement, de-escalation, and incredibly thorough preparation.

Beyond increased disorder, I am also concerned by a rise in other movements, not overtly predicated on racism or genocide (although they are frequently intertwined with those that are). Since 2008, there has been a steady evolution in anti-government extremism, from the Bundy standoff in 2014 to the militias that began appearing at alt-right protests in 2017. We've seen this before. The militia movement — a catch-all term for multiple groups and philosophies bundled by anti-government extremism and an affection for weapons — gained prominence during the first Bush administration and President Clinton's first term, when fears of a "New World Order" were catalyzed by tragic incidents at Ruby Ridge in August, 1992, and Waco in April, 1993. It culminated with the attack in Oklahoma City on April 19, 1995, which remains the second-worst act of terror in America's history. Timothy McVeigh and Terry Nichols built a sophisticated ammonium nitrate nitromethane (ANNM) bomb and killed 168 people and injured nearly 700 more. Over the next year or years, I strongly expect to see a resurgence of domestic terrorism, with new McVeighs and new attacks.

International Risks

Most of the non-economic international risks observed over the past few years show little sign of abating in 2018, even if they change shape. For example, no country is immune to the terrorism described above, and several capitols are also seeing populist movements tilt towards authoritarianism. Climate change and related or unrelated natural disasters will also continue to affect companies' operations and people. Syria will be a locus of risk in 2018 as in 2017; although combat violence may diminish, its refugee crisis may worsen if purges follow the end of open warfare. The source of the most serious potential hazards is in the East.

By purchasing power parity, China is now the largest economy on the planet, and its phenomenal growth over the past twenty years is fundamentally reordering international relationships. While the efficacy of the Obama administration's "Pivot to Asia" remains contested, the development of plans like the Trans-Pacific Partnership and AirSea Battle inarguably focused on the region from multiple vantage points. Owing to the Trump administration's lack of clarity regarding Asia policy and a dangerously shrinking State Department, that level of attention has slipped. (A word on the administration's heavy reliance on generals over diplomats for foreign policy: in each police leadership role I have had, balancing the diplomatic aspects of neighborhood policing with the more para-military aspects of targeted enforcement has been key. Imbalance negatively affects the mission.) Unfortunately, the stakes in the region are too high to lose focus.

In the case of North Korea, the stakes extend to a worst-case scenario of multi-theater nuclear war. Thankfully, this outcome is unlikely, though China's continued expansion is not. History shows that once an expansionist power sets specific goals, other nations must either stand firm or accede. In the South China Sea, the international consensus — or lack thereof — appears to offer only half-hearted opposition. (The appearance, accurate or not, that the US Navy has cut back on freedom-of-navigation operations has been noted by the media — and recent naval tragedies in the Seventh Fleet could also impact operations.) At the same time, more vigorous opposition might ultimately occasion escalations that would drastically alter the status quo, including, in an extreme case, Japan's remilitarization. In the near-East, the Belt and Road initiative will aggravate China's internal ethnic tensions in Xinjiang and may affect power dynamics with Russia, Iran, and former Soviet republics along the northern routes. In both regions, American influence is on the wane. My concern is that replacing the Pax Americana, which has treated global order as an economic public good, with a more transactional paradigm may allow disorder to fester in areas where China's national interests are not manifest. One such place that I am closely observing is the south Philippines, which is at risk of becoming the next decade's terrorist proving ground.

Cyber Capabilities Growing

Today, our technology is more advanced, effective, ubiquitous, and vulnerable than ever before. In the coming year, the Internet of Things (IoT) will continue to evolve as a source of efficiency and convenience, but also as a tool for malefactors. Just as the IoT grows, so too will the scope of distributed denial of service (DDoS) attacks. The ferocity and volume of last year's Mirai-enabled DDoS attack, which briefly shut down access to swaths of the Internet, caught our attention. However, yesterday's aberration is tomorrow's new normal. In 2018, CISOs should prepare for terabytes-per-second DDoS events. IoT devices will also continue to be avenues for network and systems intrusions. Until there is better corporate governance or stricter government regulation, IoT devices will continue to be manufactured and sold with security flaws, such as weak default passwords and insecure data-transfer protocols.

At the same time, the skillsets needed to exploit those security flaws are becoming more and more common. Ransomware as a service — the sale or easy availability of cybercrime toolkits that were once the purview of a small group of talented experts — is on the rise. Combine this with online leaks of digital vulnerabilities allegedly kept secret or developed by national intelligence agencies, and we now occupy a cybersecurity landscape where amateurs have access to immensely powerful tools — even nation-state tools. For proof, look no further than the widespread ransomware attacks that occurred with semi-regularity throughout 2017.

The cybersecurity picture has changed so much in the past six months that it is difficult to keep pace by using technology to fight technology. Instead, companies and CEOs must start focusing on the actors arrayed against them rather than the tools, because people — as well as their motives and methods — change much more slowly than apps.

Disease

A hundred years ago, a third of the world came down with the flu — and more people died from it than perished in World War I. For sheer numbers, the Spanish Flu, an influenza pandemic that hit in 1918 and 1919, is the second-most devastating natural disaster in history. (First place goes to the Black Death, in the 14th century.) Pandemics, by scope, have the potential for more catastrophic impact than any other threat. As with many other threats we have discussed, modernity has accelerated the risk. Diseases that once flared and burned out, restricted in tight localities, now travels. Zika and Ebola are just two examples of rain-forest viruses that have shown up in concrete jungles.

We are on the cusp of a pandemic now: opioid addiction. In 2016, it is estimated that the opioid epidemic took more than 60,000 lives. Although it is an epidemic, and primarily an American scourge, there are also high rates of prescription-drug abuse in Europe, China, and the developed Middle East — suggesting that an international pandemic could be coming. After all, while the American epidemic has transitioned increasingly to heroin, particularly heroin laced with the deadly synthetic fentanyl, it began with over-prescription and overuse of medical opioids. By some estimates, one of every 130 Americans has a substance-use disorder involving prescription pain relievers or heroin. If your company has more than 130 employees, then the opioid epidemic affects you.

Corporations need to be prepared for pandemics. In part, this means having plans for adjusting operations, as well as for absorbing costs associated with employees who are ill or being treated. This also means working with governmental partners, and following best practices from the medical profession. In addressing and mitigating pandemics — whether via education or vaccination, via prevention or herd immunity — stopping the spread must be a collective responsibility.

Anticipating, Mitigating and Navigating

When it comes to safety and risk, today's corporate leaders face a myriad of challenges. Smart companies are increasingly seeking to anticipate, mitigate, or navigate crises such as workplace violence, terrorism, and critical infrastructure failures or environmental calamities. Cybersecurity matters, too, because digital dangers like ransomware and data theft are on the rise. And for the sake of preparedness, I hope I've made the case for disease and disorder, as well.

Preparedness requires specific, long-term, strategic planning. For non-economic risk, this means focusing energies on under-likely, oversized events. The fact is that most people have a nearly zero percent chance of being victims of a terror attack — but there is a one-hundred percent chance that some people will be. CEOs must be ready to protect their employees and their resources — and, at times, the very brand and reputation of their companies. This includes training employees about protecting themselves and their families, and having plans in place for maintaining business operations. It includes security design and integrated physical security, and cybersecurity functions. It includes paying attention to the events and trends in the domestic and international threat picture.

The point of all this is not that the world is a risky place, although it is. The point is that the world is only a scary place if you let it be. Risks abound, but awareness and preparedness let us avoid those we should, steer through those we must, and take advantage of those we can.

Jon Murad, Managing Director, Teneo Risk, contributed to this article.

280 Park Avenue, 4th Floor
New York, NY 10017