2019 Annual Forecast

Stratfor

THREAT LENS™

Shutterstock

Threat Lens
2019 Annual Forecast

December 2018

Executive Summary

• The great power competition will cause China and Russia to intensify their industrial espionage efforts while the United States increases its efforts to stop them.

• Aggressive Iranian actions indirectly affecting, or directly targeting, its rivals' civilians and companies will intensify as U.S.-Iranian tensions rise.

• More investigations, more regulations and higher ceilings on penalties — and an unprecedented cyberthreat from the West's geopolitical rivals — will drive an increase in the number and size of penalties for organizations that suffer data breaches

Great Power Competition: The Industrial Espionage Threat

Summary: The great power competition will cause China and Russia to intensify their industrial espionage efforts while the United States increases its efforts to stop them.

Great power competition will produce a surge in corporate espionage incidents involving Western companies in 2019. The competition will drive China and Russia to maintain, if not accelerate, their already-intensive corporate espionage efforts. Chinese activity will eclipse Russia's, since China has more resources, though the United States is also more focused on countering China. U.S. companies will be the most affected target set given that the United States is the most target-rich environment for corporate espionage. The types of companies most likely to be targeted are in sectors prioritized in Chinese and Russian strategic documents.

China will be driven to engage in corporate espionage to become technologically self-sufficient and offset adverse impacts felt by a trade war and continuing U.S. efforts to cut off its access to foreign markets. Deepening financial pressure due to sanctions and a drive to make up for technological deficiencies will meanwhile drive Russia to conduct more corporate espionage. An intensification of U.S. counterintelligence efforts devoted to corporate espionage will bring more of these cases to light. The United States laid the groundwork for this initiative in November 2018, a move that will fuel a surge in manpower and resources to counter Chinese corporate espionage.

Priority Sectors of Russia and China

The two countries have identified sectors whose advancement is of greatest importance to them. Companies in these sectors are likely targets for espionage.

Sources: U.S. Chamber of Commerce, Russian Presidential decrees, The Office of the Ministry of Science and Higher Education of the Russian Federation

As a result of these trends, in 2019 we are likely to see more arrests of Russian and Chinese intelligence assets, along with indictments against officers and operatives. We are also likely to see corporate espionage activity against U.S. companies in third countries, something that arrests or warnings issued by governments will reveal. Cyber operations will also play a factor, so we will be looking for reports of cyberattacks and other forms of electronic compromise linked to China or Russia.

China and Russia will, of course, respond to the increased U.S. scrutiny, and will make the operating environment harder for U.S. companies in those countries. We expect to see hostile intelligence agencies detain or harass U.S. intelligence operatives, diplomats or civilians operating in China or Russia, such as employees of Western-linked nongovernmental organizations. Among other things, we expect them to increase their monitoring of Western business travelers and expatriates as they search for potential nonofficial cover intelligence officers.

China will be hesitant to be too overt in its response, since it still needs U.S. investment and the presence of U.S. companies. But China would be less likely to show restraint on this front if the United States were to sanction large Chinese financial institutions and tech companies, something U.S. officials have hinted they might do.

The U.S.-Iran Collision Course: Disruptions Ahead

Summary: Aggressive Iranian actions indirectly affecting, or directly targeting, its rivals' civilians and companies will intensify as U.S.-Iranian tensions rise.

The intensification of U.S.-Iranian tensions will increase the risk of aggressive Iranian action indirectly affecting, or directly targeting, civilians and companies. The United States will continue its hard-line sanctions policy while more aggressive action by Western, Israeli and Gulf Arab intelligence services will prompt retaliatory action from Iran.

The breakdown of the Joint Comprehensive Plan of Action and reimplementation of sanctions weakened moderate factions in Iran — which are more in favor of outreach to the West — and empowered more hard-line elements, including the country's capable intelligence services. This will increase the likelihood of more aggressive Iranian action, including cyberattacks, hybrid warfare and even kinetic attacks.

As a result of these trends, 2019 will see additional reports of malicious Iranian cyber activity. Iran has the intent and capability to carry out a variety of cyberattacks targeting Israeli, Gulf and Western companies. It has already laid the groundwork for such operations.

Iran plays a numbers game in its approach to cyberattacks, preferring large numbers of attacks despite a low success rate. The most threatened companies will be those with ties to the Israeli, Saudi, UAE or U.S. governments. Iran's expanding target set and capabilities mean more sectors will be at risk of everything from distributed denial of service attacks to the theft of sensitive data.

Kinetic attacks conducted by Iranian intelligence services against Gulf Arab, Israeli or Western targets or Iranian dissidents will become more likely. Iran can stir up any one of its many proxies or other groups it has links to, which could increase political unrest and attacks in their respective areas of operation. Such groups include Hezbollah in Lebanon, Popular Mobilization Forces in Iraq, militant groups in Bahrain, the Houthis in Yemen, the Taliban in Afghanistan and Shiites in Saudi Arabia's Eastern province.

Although areas where Iran has a direct presence or influential proxies are more likely to be affected, its global reach — it has attempted attacks on

five continents through its embassies and proxy networks in the last decade alone — means that action anywhere is possible. Iran also will have an incentive to take more action against Westerners in its territory to use as bargaining chips. This could include actions such as blocking the entry of Westerners, harassing them in Iran or even detaining them.

Iran Proxies and Areas of Previous Operations

Iran conducts covert actions—including assassinations, bombings and other attacks—working through its embassies and various proxies. These incidents are only a sample of Iran's activity and demonstrate the global reach of its intelligence services.

- Contains Iranian proxy forces
- Contains forces supported by Iran
- Site of successful attack by Iran
- Site of unsuccessful attack by Iran
- Site of Iranian pre-operational surveillance

The Hacking Threat: Cyber Governance

Summary: More investigations, more regulations and higher ceilings on penalties — and an unprecedented cyberthreat from the West's geopolitical rivals — will drive an increase in the number and size of penalties on organizations that suffer data breaches.

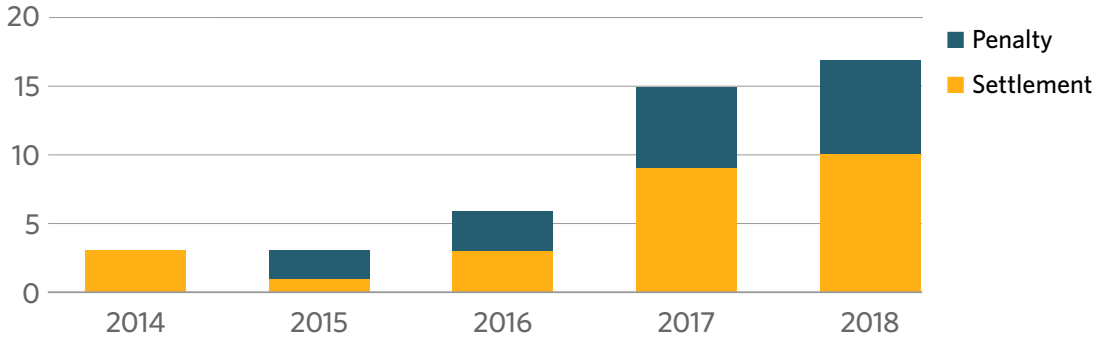
As countries like China, North Korea, Iran and Russia grow increasingly aggressive in their cyber activity, they have also increased control over their own domestic internets in order to defend them from external or internal attack. These nationalized internets are in direct contradiction to the West's continued efforts to expand the breadth and depth of internet access and connectivity around the world.

Meanwhile, the mounting threat from state-backed and criminal hackers alike has forced Western governments to respond. The United States has vowed to relax the rules of engagement when it comes to conducting offensive cyber operations and has been more public with its cyber threats, especially in the lead-up to the 2018 midterm elections. In 2019, we will see greater indications of how a more offensive U.S. cyber strategy will play out. Even so,

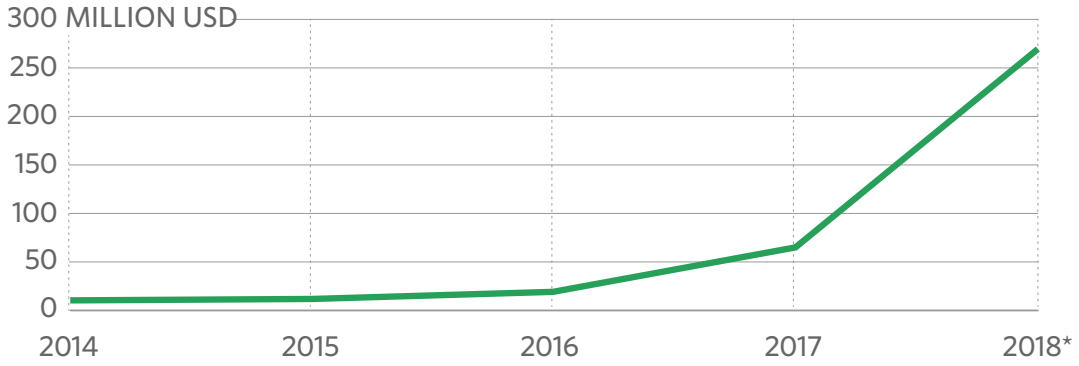
Penalties and Settlements Linked to Cyber Breaches in the U.S., UK and Canada

A study of penalties and settlements awarded following cyber breaches that compromised personal information in the U.S., UK and Canada shows that the number of cases and total losses associated with those cases are rising sharply.

Numbers of fines and settlements



Total cash awards from penalties and settlements, by year



*Through Oct. 31
Sources: UK Information Commissioner's Office, U.S. Department of Health and Human Services, Security and Exchange Commission, CBC, *Bloomberg*, *Washington Post*, Yahoo!, Reuters, *Fortune*, Topclassactions.com, NPR, Krebs On Security, classaction.org

attacks will be discreet, highly targeted and directed against the same state-backed and criminal hackers that U.S. law enforcement officials have been calling out for years.

More relevant to companies, educational institutions and other organizations is how the United States and other Western countries are increasingly shifting the liability for successful cyberattacks onto the targets. In 2018, 17 companies and organizations received fines from regulatory agencies or settled class-action lawsuits for cyberattacks that targeted them and led to data breaches. Those 17 cases cost them over $270 million in fines and settlements — a 2,700 percent increase over the amount for the three cases seen in 2014.

Given the huge role private organizations play in the functioning of the modern internet and the limited tools democratic governments have to control it, states have chosen to try to enforce good security practices on the private sector by penalizing behavior unconducive to good cybersecurity. Three main factors will drive an increase in the number and size of penalties for organizations that suffer data breaches in 2019: more investigations, more regulations and higher ceilings on penalties. The EU General Data Protection Regulation also substantially raised the ceiling for maximum penalty amounts. This means that in 2019, we could see the first billion-dollar fine levied against a company that has suffered a data breach.

Regional Viewpoints

Americas

Despite the fears of many before and after the Mexican election, constraints on newly inaugurated Mexican President Andres Manuel Lopez Obrador will prevent him from fulfilling many of his most ambitious campaign promises. Although he promised to remove the Mexican military from the war against the cartels as a candidate as did his predecessor, as president, Lopez Obrador is finding that there simply is no other option in the short term. The new administration is promoting the idea of creating a national guard to replace the military's current role, but at least on paper the national guard looks much like the former Pena Nieto administration's proposal for a gendarmerie — a proposal that did not go very far.

Promises for an amnesty for those convicted of narcotics crimes will likewise be difficult to fulfill. The plan would only apply to individuals not involved in violent crimes such as murder, kidnapping, extortion, etc., but there are quite simply no cartel groups that do not engage in such activity. The real hope for Mexico's future with the Lopez Obrador administration rests in his pledge to aggressively address corruption. Corruption at all levels of government is what has empowered Mexican criminal groups to become so powerful and brutal, and if the new government is able to address corruption, it could go a long way toward changing Mexico's security environment for the better.

Meanwhile, the ongoing collapse of Venezuela will continue to create a relatively safe area for criminal enterprises to operate — and a dangerous area for everyone else. The hard line taken against Colombia's militant groups and the continued loss of confidence in the peace deal will continue to push guerrilla and criminal groups out of Colombia and into the border regions of surrounding states, including significant amounts of Venezuelan territory.

Militant and criminal groups operating on the periphery of most northern Latin American states will continue to hamper cross-border commerce, and will likely become active across large areas of rural northern Brazil. As increased criminal activity becomes a threat to the security situation in the region, it will draw a stronger response from the new government of Jair Bolsonaro, which will likely shift security assets to the northern regions to counter cross-border criminal groups. Increased pressure from security forces will likely invite retaliation from militants targeting the Brazilian state and private enterprise. Conflict is unlikely, however, to spread beyond the border zones.

Asia-Pacific

While China and the West are locked in an espionage/counterespionage struggle, Beijing will also be testing U.S. influence in East Asia in several key spots: the Korean Peninsula, Taiwan and in China's own domestic economy. The North Korean deal will hold through 2019, but U.S. demands for tangible moves from North Korea will clash with South Korean efforts to keep the peace. The gap between South Korea and the United States gives China an opportunity to exploit, making the U.S.-South Korea alliance more complicated. And Taiwan will continue to be a hot spot in the China-U.S. rivalry. Promises from Washington to bolster its relationship with Taipei risk retaliatory measures from Beijing ranging from unfavorable economic treatment to increased military patrols in the South China Sea.

As the trade war between the United States and China continues into 2019, Beijing has avoided carrying out major retaliation against U.S. companies operating in China, opting instead for a strategy of economic reforms to drive domestic production and consumption. U.S. companies should still be aware of the business continuity risk posed by anti-U.S. sentiment fueled by the White House's more aggressive policies toward China.

Eurasia

Russia's strategy of hybrid warfare against the West is set to continue in the form of cyberattacks, disinformation campaigns and physical operations around the world, in addition to its continued intelligence efforts outlined above. Its most likely targets will be fault lines on key issues such as EU sanctions against Russia, support for which Italy is threatening.

EU parliamentary elections in May will present major opportunities for Russia to move opinion more in its favor, or at least to roil political stability enough to cause distractions. Moldovan elections in February and Ukrainian elections in March will also provide Russia the opportunity to achieve political victories in its so-called near abroad through potentially disruptive tactics.

Europe

British membership in the European Union will end March 29, 2019, at which point the parties will have to reach a withdrawal agreement to manage the separation over the subsequent two years, or the no-deal scenario will kick in. The most likely scenario is that a withdrawal agreement will be reached before the deadline, preventing immediate or sudden disruptions at border crossings. But this will be a complex process worth monitoring in case it derails. Even in the event of a no-deal scenario, we forecast that both the European Union and the United Kingdom will be motivated to minimize disruptions at their mutual border.

The debate over withdrawing from the European Union will also continue to spur political unrest. Brexit supporters will likely continue to protest paying EU obligations and any other compromises in the agreement. Anti-Brexit protesters will likely continue demonstrations to try to force a popular referendum on the agreement, or in a highly unlikely scenario, a vote to reverse Brexit.

French President Emmanuel Macron will attempt to reform France's pension system by streamlining the current system and raising the retirement age. Given the sensitivity of pension systems in Europe and particularly in France, such reforms are certain to spark a backlash and protests. We expect massive rallies in cities across France, strikes, disruptions to transport infrastructure and disruptions to supply chains. While strikes and protest activity in France are fairly common, these have the potential to be the largest since the 2010 strikes over a rise in the retirement age, which saw millions of public sector workers stop work over a dozen times throughout the year.

Middle East and North Africa

Saudi Arabia will continue to court foreign investment and attempt to make itself more hospitable for foreign companies. The aggressiveness of recent Saudi foreign policy has drawn scrutiny from the United States and Western countries, however, and has increased the reputational risk for companies doing business there.

Geopolitical factors will ensure the U.S.-Saudi strategic relationship will remain in place, even if it has been temporarily rattled. A key signpost to watch will be the outcome of the U.S. Magnitsky Act investigation, which has a deadline of Feb. 7 (although it could end earlier), to see how far the United States will go to punish Riyadh for the death of Jamal Khashoggi.

Relations between Turkey and Western countries will gradually improve after a year of upheavals. Ongoing points of contention may cause occasional diplomatic spats, which could lead to upticks in anti-U.S. and anti-European sentiment in Turkey. But all sides will seek to mitigate any damage and ensure that relations do not rupture.

South Asia

Afghanistan's security environment is unlikely to improve, and the central government will struggle to stabilize itself. The United States will likely maintain its military strategy in Afghanistan. The Taliban will meanwhile use its momentum to wear down U.S. resolve, and the Islamic State's Khorasan Province will exploit the ongoing instability.

The run-up to Indian elections in April or May will see increasing disruptions from political unrest, with the ruling Bharatiya Janata Party pushing a Hindu nationalist agenda, opposition coalescing against it and various political constituencies jockeying for candidates to advance their agendas. A focus by the central government on security in the run-up to the elections will also increase the risk of attacks, clashes and other militant activity in traditional security hotspots, including Jammu and Kashmir state as well as in Chhattisgarh state, with the potential for spillover into neighboring states.

Sub-Saharan Africa

South Africa's parliament is poised to pursue constitutional reform concerning land expropriation in 2019. The reforms are more part of the African National Congress's bid for re-election in 2019 than out of any real desire for widespread land redistribution. Foreign investors are already spooked, and the government does not want to risk scaring them off altogether through indiscriminate land expropriation. ☐

Threat Lens

The only unified solution that integrates the full spectrum of issues facing security leaders, spanning threats against people, infrastructure, intellectual property and business continuity.

Contact

threatlens@stratfor.com

www.stratfor.com/threat-lens

+1 512 744 4300, Option 4

+1 855 804 7408, Option 4

Stratfor