REPORT

2024 GLOBAL SECURITY OUTLOOK: A NEXUS OF DISRUPTION

The Intersection of Cyberattacks, Political Polarization, & Regional Conflict

CHIEF EDITOR Karna McGarry

CONTRIBUTING AUTHORS Ryan Barnett, Garrett Bell, Robert Collie, Julien Dresbach, Steven Duke, Omar Elshamy, Wagner Horta, Chad Kunkle, Nicholas Nemtuda, Emily Paglicci, Claudia Santillanvazquez, Michael Searway

MESSAGE FROM THE CEO

KRIS COLEMAN
FOUNDER & CEO, RED5

I am proud to share our comprehensive exploration of the dynamic risk landscape that shapes our world today — the *2024 Global Security Outlook: A Nexus of Disruption report*. Authored by our team of dedicated analysts, this white paper delves into the critical developments and potential challenges that lie ahead in the realm of global security.

In an era where rapid technological advancements intersect with geopolitical complexities, understanding the intricacies of emerging threats is paramount. Our analysts have meticulously examined the evolving landscape, identifying trends that will define the security environment in the coming year.

As we navigate through this complex terrain, it is imperative that we stay ahead of the curve, and this white paper serves as an invaluable resource in that endeavor. I encourage each of you to engage with the insights presented, fostering discussions that will enrich our collective understanding and inform our strategic decisions.

K. Coleman

TABLE OF CONTENTS

02.
ABOUT RED5 AUTHORSHIP

03.
EXECUTIVE SUMMARY

05.
REGIONAL CONFLICT

12.
CYBER ATTACKS

16.
POLITICAL POLARIZATION

ABOUT RED5

ABOUT US

Our purpose is to ensure bad things don't happen to good people. We leverage our depth of expertise and capabilities to deliver security and risk management services that protect clients from both known and unknown threats.

The excellence of our entire team is driven by robust and diverse backgrounds across agencies, the private sector, and public sector organizations. Red5 consists of individuals who are recognized within their networks for solving problems others couldn't. We establish strong partnerships with our clients to ensure safe and successful results.

WHAT WE DO

Red5 provides comprehensive managed service solutions for threat monitoring, privacy, and intelligence services.

We're always there to protect you, even when you don't notice. Our analysts use industry-leading intelligence tools and best practices to give you expert-led **security intelligence, threat monitoring**, and **privacy solutions**.

5 CORE TENETS

- **Confidentiality**
- **Authenticity**
- **Responsiveness**
- **Rigor**
- **Agility**

Executive Summary

2024 Trend Toward Regional Conflict

Red5 analysts assess that 2024 will see an increase in disruption to business operations due to escalations in regional conflicts, continued cyberattacks, and political polarization and civil unrest being magnified using artificial intelligence (AI) and disinformation.

Global business operations will likely be disrupted in 2024 as a direct result of conflict and territorial disputes in Eastern Europe, Latin America, Southeast Asia, and the Middle East. Countries, such as China, North Korea, and Iran, may attempt to increase their influence in 2024 through antagonizing efforts, due to the West's preoccupation with conflicts in Ukraine and Gaza.

Cyber Attacks

Cyber threat actors will utilize AI to conduct increasingly complex cyberattacks against businesses and critical infrastructure in 2024. AI malware can increase a cyber threat group's rate of success by mimicking desired behaviors and bypassing conventional network protections. Cyber threat groups affiliated with Russia, China, and Iran will continue to target private corporations and national critical infrastructure to attack soft targets without international retaliation.

Executive Summary

Political Polarization

Political polarization probably will intensify in several countries in 2024, posing increased security risks for enterprises. The coming year will see increased use of AI tools to spread disinformation that will likely further aggravate polarization. Corporations perceived to be involved in the development of AI will face heightened security risks in the coming year.

- Countries with national elections, such as the United States and India, will face increased risks for political violence in 2024, due to deepening social divisions.

- The Middle East and North Africa faces an increased risk of political violence, due to the ongoing Israel-Gaza conflict.

Trend Toward Regional Conflict

Red5 expects an intensification of regional disputes to occur in 2024, due to an uptick in political and military action to control disputed territory. Regional disputes turning to conflict have been trending upward since late 2022 and will likely continue in 2024. Actions taken by Russia, Israel, and Venezuela illustrate a broader trend toward regional conflict.

Multiple geopolitical disputes turned to conflict in 2023, which may embolden other countries to engage in disruptive operations in 2024. Iran, China, and North Korea are likely to see an opportunity to increase the influence—either regionally or elsewhere—while the West is preoccupied with existing hotspots.

- The Israel/Hamas and Russia/Ukraine conflicts both elicited a strong Western response through support of one side. The outcome of the conflicts in Ukraine, Gaza, and Guyana may embolden countries, such as Iran, China, and North Korea to increase disruptive operations and enhance their regional influence.

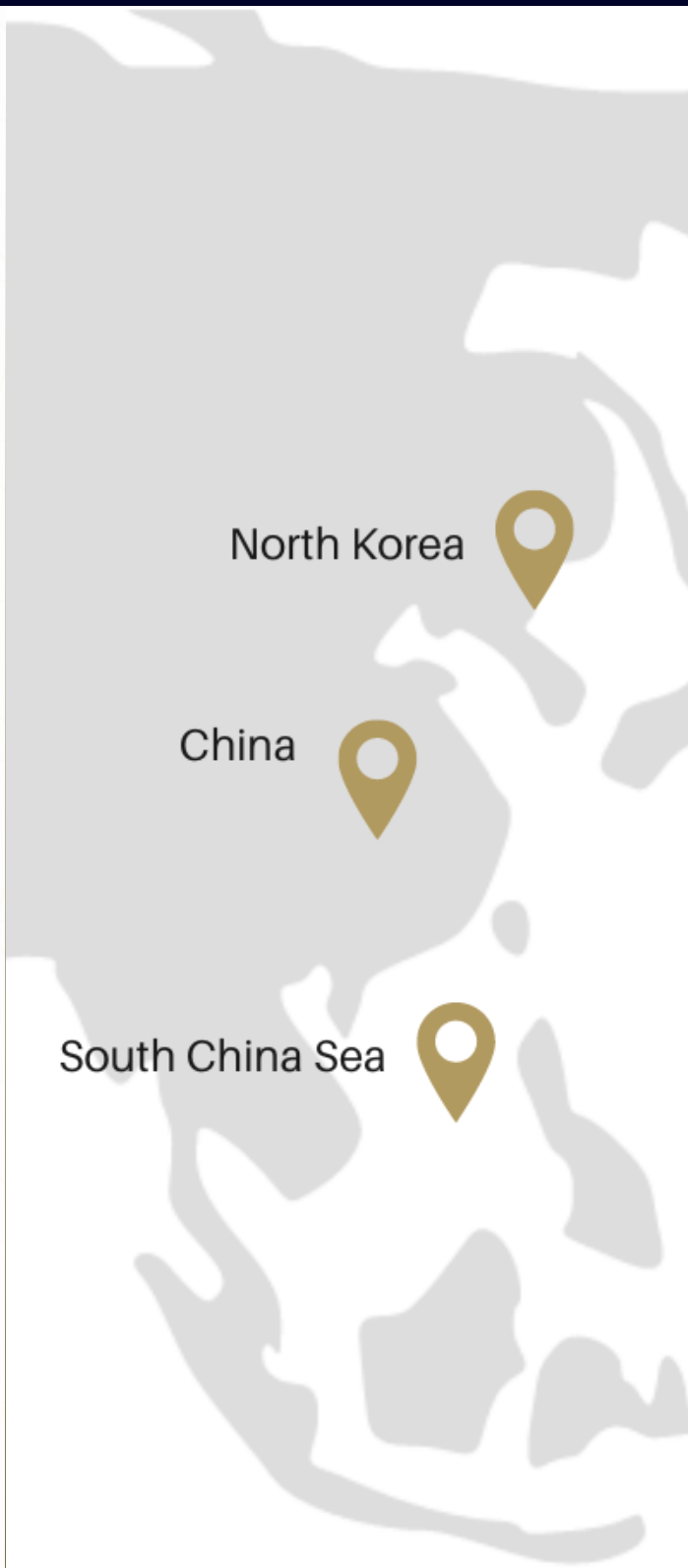
Red5 security and intelligence analysts assess that China, North Korea, Russia, and Iran will use familiar tactics of increased rhetoric and disruption efforts to further their political and economic agendas.

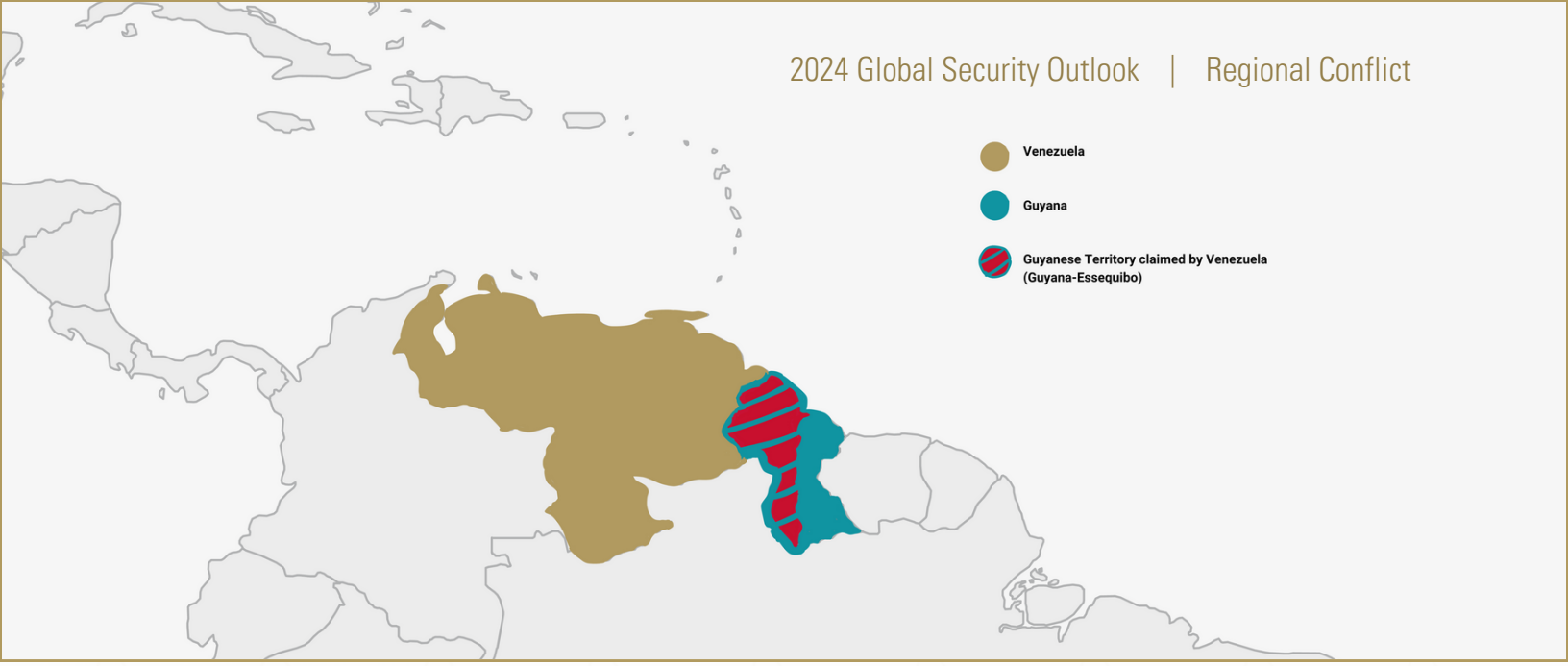
China's actions in the South China Sea risks dragging regional allies into the confrontation.

China will likely be emboldened to increase its influence in the South China Sea in the coming months. China has increased its antagonizing interceptions of military, private, and commercial ships, and aircraft in international waters. The People's Liberation Army aircraft have been intercepting military aircraft at increasingly close range. Similar actions will continue to occur as China seeks to deter adversarial actors from operating in the South China Sea where trillions of dollars of global trade flow through each year.

North Korea probably will view ongoing conflicts as an opportunity to amplify disruption efforts. North Korea will continue to seek disarray, which it can achieve through the political and financial support of governments and organizations that are being punished by Western governments.

- Kim Jong Un in late December 2023 publicly called for the annihilation of the US and South Korea if provoked and subsequently committed to further weapons testing and defense spending.





Venezuela nears land grab of oil-rich region of Guyana, risking a limited scope land war in Latin America. President Nicolás Maduro will likely use diplomatic pressure and brinkmanship—bolstered by the US's distraction in the Middle East and Ukraine—to try and obtain resource access to the Essequibo region of Guyana.

- Venezuelans approved a referendum by over 90% in late December 2023 to annex the region.

- Brazil, as of late December 2023, had moved additional forces to the border with Guyana. Brazil supports the internationally recognized Guyana sovereignty, which may serve as a deterrence to Venezuela starting a land war with Guyana.

Venezuela's oil industry is nationalized, which would result in the seizure of operations of foreign oil companies in the region and likely lead to major disruptions in the oil and gas industry. In late 2023, the US completed a prisoner exchange with the Venezuelan government, which resulted in the release of 10 detained Americans and 21 Venezuelan political prisoners. The agreement may be seen as an effort to ease US-Venezuelan tensions because of Maduro's claims of annexing Guyana Essequibo.

Geographical conflicts elevate security risk landscape

Ukraine-Russian conflict two years in tests support for political and financial capital from allies

The war in Ukraine is unlikely to end in 2024, as Ukraine and Russia have not met their strategic goals and appear unwilling to negotiate peace. Russia's actions in international negotiations and increased military spending show it has no desire to de-escalate and exit Ukraine in the near term. The Kremlin will likely escalate the conflict to bolster national unity before the Russian presidential elections in mid-March and to divide western support during the US presidential election in November 2024.

The Russian government is trying to outlast Western military aid to Ukraine. Russia has increased its military spending as the conflict has dramatically slowed to a war of attrition as both sides have entrenched themselves. Russia conscripted an additional 130,000 soldiers for training, indicating that the Kremlin still seeks its strategic goal of annexing all or part of Ukraine.

- Russia sees the waning support in the US Congress as a sign that financial support to Ukraine will dwindle in the coming months.
- The loss of financial support in 2024 would coincide with Russia's winter offensive, which will likely continue into March 2024.

Russia's withdrawal from international negotiations has prolonged the war in Ukraine and impacts supply chain for goods, food, and energy. Russia will continue to blockade Ukrainian shipping efforts in the Black Sea to increase transportation costs and economically weaken Ukraine. The EU, in response, probably will restrict gas and oil imports to economically weaken Russia. Russia withdrew from the Ukrainian grain deal and refused to conduct further negotiations with Ukraine in 2023.

Regional actors walk high-wire act of containment within Middle East

A confined conflict between Israel and Hamas will likely result in limited harm to the global economy. In the event of wider regional spillover, impacts to the global economy and security environment would be significant. Actors in the region such as the Houthis, Hezbollah, and other Iranian proxies have increased attacks against Israeli and US assets within Syria and Iraq. Attacks against commercial and military vessels in the Red Sea continue. If Western aid to Israel continues, then Iranian-backed groups may look to escalate hostilities. This would have serious impact on commercial entities and result in additional attacks against commercial shipping vessels, attacks against oil refineries, and other Western commercial interests in the Middle East.

- ***A contained Israel/Hamas conflict would have a limited impact on the global economy.*** Oil production and major global shipping routes would likely be minimally impacted by the conflict in Gaza. Western response to Iranian-backed groups attacking military assets in the region has elicited limited military response by the West in an attempt to avoid escalation and greater regional spillover.

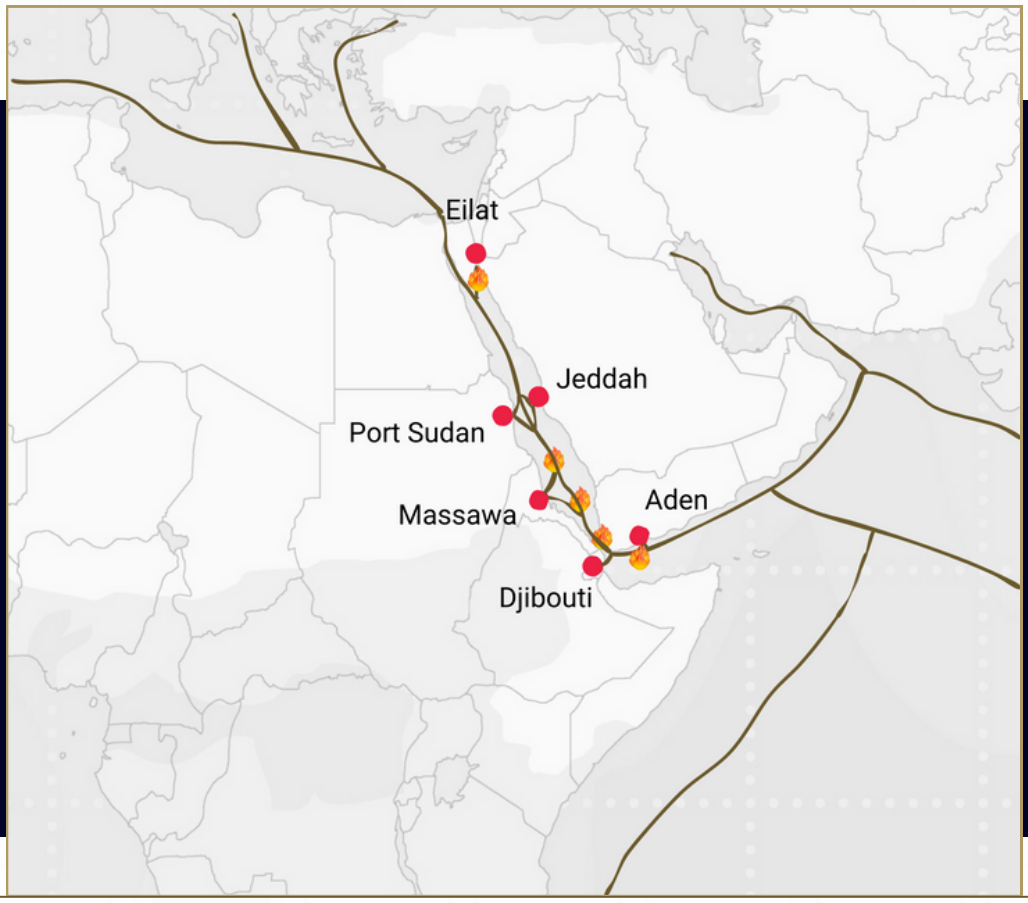
- ***An expanded regional conflict would likely cause significant impacts to the global economy and security environment.*** Iranian participation—through its proxies—will lead to further attacks on US regional facilities, major shipping routes, and oil refineries in 2024 by Iranian-backed groups in the region.

Houthi aggression risks broader regional conflicts

Houthi acts of aggression against internationally flagged ships risk pulling the Saudis back into conflict. The Saudis are committed to retaining international investment and businesses to bolster their economy, while simultaneously maintaining diplomatic advancement within the region, particularly with Tehran.

- The US military ratcheted up their response to Houthi activity, hitting Houthi targets in early 2024. The US navy in late December 2023, destroyed Houthi small boats after being fired upon by the Houthis who were attempting to board a container ship in the Red Sea.

- The Houthi attacks have targeted commercial vessels flagged to the US, Norway, Hong Kong, Singapore, Panama, Liberia, Cayman Islands, Gabon, Marshall Islands, Malta, Cyprus, and the Bahamas.



There have been more than 30 hostile incidents involving Houthis and commercial shipping vessels in the Red Sea since mid-November 2023.

REGIONAL SPOTLIGHT

Iran is interested in disruption without triggering an outright conflict, but risks a proxy war in the region.

Iran remains active in the region and still uses its preferred weapon of choice—its proxy groups. Iranian opportunity to use proxies to strategically engage with regional disputes that allows it to hit its adversaries while not risking an all-out war or confrontation with either the US or Israel. Iranian proxies include the Houthis attacks ships in the Red Sea, Kataib Hezbollah targeting US bases in Iraq and Syria, and Lebanese Hezbollah along the Israel-Lebanon border.

The recent attacks against Hamas leadership and within Iran highlights the risk of proxy wars. The use of proxies is a way for countries to provide disruptive events without engaging at the state level, however, the risk of violence and civilian casualties is high.

- Company security officers with operations in MENA or personnel who travel to the region would be well positioned in 2024 to face the increased risk levels by using travel risk reports, emergency evacuation plans, and business continuity plans.

Iranian proxies include:

- Houthis attack ships in the Red Sea
- Kataib Hezbollah targeting US bases in Iraq and Syria
- Lebanese Hezbollah along the Israel-Lebanon border

Cyber Attacks

AI will enable threat groups to increase the frequency and complexity of cyber attacks in 2024. Red5 intelligence and security analysts assess those regional conflicts and key countries with national elections in 2024 increases the risk for cyber-attacks targeting corporations and critical infrastructure.

Cyber threat groups will increase their use of AI in 2024 to exploit vulnerabilities and gain unauthorized access to vital networks. In 2023, AI was used in phishing attacks, malware, and disinformation campaigns. AI campaigns can increase threat groups' rate of success, as AI can quickly analyze and adapt to reach a wider audience, mimic desired behaviors, and bypass obstacles, potentially at a faster pace than security teams' responses. Cyber threat groups affiliated with countries such as Russia, China, and Iran will try to target US corporations and critical infrastructure to further their political, economic, and military strategic goals in 2024.

Russia will attempt cyber intrusions aimed at election infrastructure, political parties, and media companies to disrupt US and European support for Ukraine and to increase political violence during US and EU elections in 2024.

Iran will continue to target US and Israeli critical infrastructure in response to the Israel-Hamas conflict. The Iranian Revolutionary Guard Corps probably will use their cyber proxies to try to infiltrate US critical infrastructure, technology, biotech, or healthcare companies to disrupt energy supplies and international supply chains.

China will likely expand their intrusions into technology, pharmaceutical, and energy industries to conduct cyber espionage and to bolster their cybersecurity advantage if US-China relations decline further in 2024.

Corporations and corporate executives, especially those within critical industries like technology, energy, biotech and healthcare, and defense, are the primary targets of cyberattacks and corporate espionage. The targeting objective include disruption, extortion, intellectual theft, and reputational damage.

Large technology and social media companies are likely targets, as breaches or compromises of their data may be used to facilitate espionage or disinformation by actors like Russia and China.

Proactive Measures for C-Suite Teams

AI enhanced cyberattacks presents a threat to corporations and their C-suite by increasing the overall security risk environment surrounding personnel, physical locations, and operations.

- Corporate entities must take proactive measures to avoid becoming “soft targets” for these cyber campaigns.
- Corporations should review their C-suite's online exposure to reduce their digital footprint, monitor for impersonation accounts, and include social media monitoring to mitigate the risk of physical and reputation harm.

REGIONAL SPOTLIGHT

Russian state-sponsored cyber groups will likely utilize AI in the upcoming 2024 US presidential election to help manufacture social media posts that are up-to-date and overwhelming in number.

Kremlin-sourced social media profiles could attract large followings by reposting mainstream news sources. Russian interference will not be limited to the United States. Following the November 2023 local elections in Moldova, the Security and Intelligence Service of Moldova claimed that Russia had launched a disinformation campaign in the country. Russian interference in global elections will remain a continuing trend in 2024.

Russian retaliation for US assistance to Ukraine will continue to be a major concern, with greater potential for cyber-attacks aimed at election infrastructure.

Russia remains a top cyber threat, according to the Office of the Director of National Intelligence, as US agencies continue to see evidence of its sponsored APTs (advanced persistent threats) launching ransomware and malware attacks. Russia is likely to attempt to diminish US citizens' support of democratic institutions through election interference.

Kremlin-based election interference will likely branch out to advance its agenda globally, particularly in countries where Russia already holds some level of political influence:

- Venezuela
- Sub-Saharan Africa
- Central Asia
- the Causasus
- Eastern Europe

& more.

Companies remain vulnerable to China's espionage efforts against C-suite and leadership

China will remain a major cyber threat actor with a sustained focus on industrial espionage rather than critical infrastructure attacks. Rising tensions between China and the US regarding contested territory in the South China Sea, particularly Taiwan, would impact key trade routes and semiconductor chip manufacturing. Taiwan accounts for more than 60% of the world's semiconductor chip production and 90% of the most advanced semiconductor chips.

China's infrastructure development in Central Asia, Africa, and the Middle East, as well as projects in Latin America, such as 5G telecommunications, require expansions in China's manufacturing and technical capacity. China's industrial espionage efforts is used to further its efforts and competitive edge. Companies working in these sectors or regions—whether as a competitor or partner with China—are at some risk of industrial or corporate espionage.

- Companies and C-suite members are at risk of corporate or state-sponsored espionage efforts by China while traveling or in their home countries.

- Enterprise security programs will need to educate their C-suite members to the need for counterintelligence briefings, monitoring online exposure, impersonation accounts, and phishing campaigns.

The Threat of Political Polarization and Disinformation Fueled by AI

Political polarization will continue to intensify in 2024, posing increased security risks for companies operating in area with civil unrest and upcoming elections and the deployment of AI technologies will magnify the risk. The increased uptake of AI tools for spreading disinformation, including other factors, are driving a global trend for intensifying polarization.

- Companies may become increasingly targeted by AI disinformation. Enterprises involved in the development of AI technologies will face heightened security risks in 2024 due to AI's persistently controversial nature.

Increased levels of political volatility will raise the risk for political violence, which may impact the overall security environment of companies operating in these areas. High level of civil unrest, protests, and acts of vandalism can disrupt companies' operations and may directly risk employee safety.

- Corporate enterprises may also be targeted by political organizations or actors based on the consumers' and policymakers' political opinions.

Country-specific conditions will be the decisive factor for the risk of political violence across the world. Rising global levels of polarization and unrest will not affect all countries equally and are influenced by varying factors in different places. Political violence is more likely to occur in countries with entrenched divisions between social groups and a history of violence between them. Major political elections are a catalyst for large-scale protest activity, which can turn violent. Other factors—the economy, rise of populist movements, entrenched social divisions, and active conflicts—also impact the overall risk for civil unrest.

The United States is at an increased risk of political violence relative to past election cycles. A combination of a persistent upward trend of political polarization, the weaponization of emerging technologies by domestic and foreign political actors, and the 2024 presidential election are likely to instigate varying levels of online harassment, social media outrage, and political violence.

- C-suite members and companies that publish official stances, practices, or policies tied to certain political parties or candidates will face a higher risk of political backlash due to those associations. This may include online harassment, doxing incidents, threat of physical violence towards the C-suite member, their family, or residence.

The Middle East and North Africa (MENA) region is at an increased risk of political violence, driven by the Israel-Hamas conflict. The Israel-Hamas conflict has already resulted in spill-over effects in the region. Iranian proxies serve their purpose to disrupt and undermine cease-fire efforts, while simultaneously striking Western targets in the region. The Saudis are attempting to keep Houthi aggression in check, without harming their status in the region. The conflict, meanwhile, provides rallying cries for religious or sectarian parties to gain supporters.

Countries in the European Union will be more susceptible to nationalist movements in 2024. E.U. members will continue to experience backlash against its policies regarding migrants. Geert Wilders' right-wing, populist party's success in the 2023 Netherlands General Election could be indicative of the trend toward nationalism. A similar trend may be seen in more prosperous northern and western countries, including Sweden, Norway, Denmark, Germany, and France.

- Companies operating in the EU may be faced with physical security risks for their personnel or operations, if national movements spark anti-immigrant protests, labor disputes or strikes, or protests aimed at the host-country government.

Elections in India will suffer political violence, and the results of upcoming elections in Taiwan will possibly have global implications on computing and information technology. India is set to hold its general election in the first half of 2024. In the past five years, Hindu nationalists have started to target Muslim minority groups in the country. This trend of violence against Muslims will likely continue, as Prime Minister Narendra Modi and his Hindu nationalist party enjoy high popularity.

- Companies with a labor force in India, should monitor for increased in rhetoric against Muslims, attacks against communities, and targeted threats against employees.

Taiwan's presidential election in January 2024 will set the stage for the new government's stance to counter an increasingly aggressive China. The rhetoric and results of the elections in 2024 will possibly provoke the Chinese Communist Party, contributing to rising tensions between both countries. Taiwan's future elections could have an impact on the global supply of semiconductors. Although the political status quo of the country is likely to be maintained, the results of the election will be consequential for global semiconductor supply chains if China decides to signal its displeasure with the new government or make a show of force.

- Companies with personnel and operations in Taiwan and China should review business continuity operations and emergency evacuation planning for 2024 to prepare for potential changes in the security landscape.

AI technologies will increase disinformation and magnify political fracturing

AI technologies likely foment political polarization and violence to varying extents in 2024, posing new security risks for corporate enterprises.

- ***AI-powered tools, such as deepfake and text generators, have created a powerful and often cheap avenue for manipulating public opinion.*** In 2023, for example, Venezuela and China used video deepfakes to spread propaganda, circulating it to foreign audiences.

- ***AI disinformation has also been used specifically to influence political elections.*** In 2023, deepfake videos and images smearing candidates were employed in multiple countries, including the United States, Turkey, Slovakia, and Nigeria. Upcoming high-profile elections in 2024, such as the general elections in the United States, India, and the European Parliament, will likely be targets for AI-generated disinformation.

- ***India is one country at a high risk of suffering from the spread of AI disinformation in the coming year,*** due to its upcoming elections, entrenched ethnic and religious divisions, and a robust social media scene that online platforms have often struggled to moderate.

Enterprise operations are at risk to be significantly affected as AI becomes a more common tool for their adversaries. Businesses are likely to become common targets for AI-powered disinformation and attacks in 2024. The adoption of AI tools by political actors signals an era in which these technologies are evolving from niche to widespread application, and the corporate sector will be affected. Companies will be impacted by AI-powered cyberattacks and scams, and also by smearing and impersonation campaigns using AI-generated content.

A Note for C-Suite Teams

Enterprises directly involved with developing AI technologies or moderating AI-based content will see security risks increased in 2024.

Controversy surrounding the usage of AI technologies will continue to increase in the 2024. Companies involved with AI probably will see an increase in the incidence of lawsuits, public protests, and violent threats. This risk will be exacerbated if there is a growing public sentiment that these companies are not doing enough to responsibly develop or moderate AI technologies.

- C-suite members face reputational harm because of AI-generated content, such as videos and stories.
- Impersonation accounts can result in reputational harm, online harassment, and threat of violence against C-suite members, Board members, or personnel.

How Red5 Can Help

Escalating global security trends highlight the need for corporations to be well-informed of the unique threats they face, which are multiplying in an increasingly uncertain and unstable world.

Red5 analysts leverage their in-house expertise to proactively monitor the global threat space to remain well-informed, decipher ambiguous security challenges, and produce tailored and actionable security solutions for our clients. Our analysts use industry-leading intelligence tools and best practices to give you expert-led managed security intelligence, threat monitoring, and privacy solutions.

Managed Intelligence & Analysis

- Expert-led monitoring, analysis, and insights
- Flexible investigations and reports, adaptable to changing needs and risks
- Monitor for threats across mainstream and alternative social media

Managed Threat Monitoring

- Remove fake or impersonation accounts
- Dark web surveillance for compromised credentials
- Geofenced monitoring of location-specific threats

Managed Privacy Solutions

- Understand the full-picture of your digital footprint and how to minimize risks
- Remove your personal information as quickly as its bought, sold, and shared with WebScrub
- Protect against common attack tactics, hacking attempts, scams, and spam

GET IN TOUCH TO LEARN MORE


red5security.com/contact-us


info@red5security.com