April 9, 2025

White Paper

GEOIntelligence

There are many global threat vectors that challenge the United States. In terms of the worst potential consequence to the United States, the foremost threat is if the United States becomes involved in a conflict with Russia and/or China, which could then escalate into an existential nuclear war – fortunately, this threat is very low today (but likely increasing in the coming years). Other threat vectors come from countries such as North Korea and Iran – they pose serious threats to regional stability, but do not pose an existential economic or security threat to the United States. While also not an existential threat, Violent Extremist Organizations (VEOs) and Transnational Criminal Organizations (TCOs) remain significant national security concerns for the homeland and U.S. interests abroad.

The Trump Administration places a high priority on homeland defense and securing the borders. In this vein, expect aggressive action by the Administration to address VEO and TCO threats. In his first term, President Trump initiated a long-term operation in Iraq and Syria to set back large gains made by the Islamic State, killing thousands of terrorists and freeing large tracks of land from their grip. Early in his second term, President Trump ordered U.S. forces to decisively strike Houthis in Yemon, an Iranian VEO proxy, to restore freedom of navigation in the Gulf of Aden and the Red Sea. In terms of TCO threats, President Trump, in his recent Joint Address to Congress, highlighted that the drug cartels South of the border are now prioritized as terrorists, on par with the Islamic State and other terror organizations, also saying that they pose “a grave threat to our national security.”

VEOs and TCOs have existed for decades, but they are sometimes underappreciated in terms of the enduring threats they pose to U.S. homeland security as well as regional stability in the areas of the globe where VEOs and TCOs enjoy a base of operations, haven, and sanctuary.

It bears acknowledging upfront that domestic terrorism threats also exist from groups such as fascists and white supremacists and could be considered VEOs and/or TCOs. This report, however, focuses on foreign VEOs and TCOs, providing an overview of their background, current state, and potential future implications to enable leaders to better understand these growing threats at the nexus of national and international security, economic interests, and corporate risk.

Violent Extremist Organizations:

“Terrorism” as a term came into use during the French Revolution, though the phenomena of terror-inspired acts probably dates back to antiquity. There is no universally agreed upon definition for VEOs, but here is a working definition: “groups of people who support or commit violence to achieve ideological, political, or religious goals.” Unlike warfare, there are no rules with respect to the methods of violence, targets of violence, or the scope and scale of VEO operations. These factors often expose civil society and security forces greatest vulnerabilities to VEOs.

David Rapoport, in his book Waves of Terrorism: from 1879 to Present, describes terrorism using a generational model with Anarchists (1880s - 1920), Anti-Colonialists (1920 - 1960s), The New Left (1960s - 1970s), and Religious-based terrorism (1979 - present). Within this construct, he highlights that while terrorism is not new, global visibility shifted sharply to focus on combating terrorism because of the 9/11 attacks. That focus has lasted for nearly 25 years as the world's best Western and free market nation militaries, led by the United States, fought wars in Afghanistan, Iraq, Syria, and other regions as well, involving coalitions of up to 50 nations focused on various VEOs. Despite the human and economic cost of the U.S. involvement in all three of these conflicts, the VEO ideology of Al Qaeda (AQ), the Islamic State (IS), and other religious extremist groups have persisted. The cost of U.S. involvement has been tremendous, foremost with the loss of thousands of U.S. warriors with many more wounded and in terms of dollars, upwards of $8 trillion to date. The twenty-plus years of U.S.-led counterterrorism operations against VEOs have also impacted U.S. conventional force readiness, and the ability to build and sustain readiness for large-scale combat operations against one or more of the U.S. strategic competitors.

The impact of violent extremist actions has enduring regional and global adverse impacts. The United States' 9/11 and Israel's 7 Oct, combined with the countless acts of terrorism in the two-plus decades in between these catastrophic attacks, provide stark and lasting reminders of the strategic consequences of complacency against VEOs. VEO threats to nations and the global order are not going away.

The resilience of VEOs rests with their extremist ideologies, particularly among disenfranchised or impoverished populations where extremist ideologies incubate among populations where there is no security, governance, or economic opportunity – VEOs exploit the vulnerable. These organizations also tend to be highly centralized in planning terrorist attacks to enable achieving their ideological and political aims. They operate in a decentralized manner and often are widely dispersed. The nature of VEO operations, particularly spectacular attacks, are creative, indiscriminate, and often unpredictable. Many VEOs are well funded, highly trained, and equipped, also leveraging safe havens in ungoverned spaces globally and often enjoy sanctuary among ideologically aligned States, such as Pakistan and Iran.

When left unchecked, both VEO (and TCO for that matter) networks can become so vast and complex that a global campaign is necessary to dismantle the human and physical infrastructure of a Violent Extremist or Transnational Organization. The exact circumstances that led the United States to declare a global campaign against Al Qaeda following the attacks of 9/11.

The predominant VEOs globally are Islamic extremists of the Sunni or Shia branches of Islam. Sunni and Shia are defined by their interpretation of Islam and its place in the world, achieved through Global Jihad with the ultimate objective being Sunni or Shia Islam as the global religion and Sharia Law as the form of religious governance. Both Sunni and Shia VEOs rose to national and international recognition starting in 1979 – the Sunnis through its loose coalition to combat the Soviet invasion of Afghanistan and the Shia as an outcropping of the Iranian Revolution and the ensuing Iran-Iraq war of the 1980s.

For general context, Sunni and Shia Muslims are the two major sects of Islam representing ~85% and ~15% respectively of Muslims globally. Sunni Muslims are generally aligned with one of three political approaches: Quietism (these groups tend to be apolitical), Political Islam (such as The Muslim Brotherhood), and Jihadi (this includes AQ and IS). In terms of centers of the movements, Saudi Arabia, the home of Mecca and Medina is largely seen as the lead Sunni Muslim nation in the world, contrasting with Iran, which is considered the lead Shia Muslim nation in the world.

Sunni VEOs:

Since 1979, two main groups of Salafi-Jihadists have emerged and remained, AQ and IS. Both have strong anti-Western and anti-Israeli views; however, they do not share the same perspectives. According to Fred Kagan and his team of scholars in U.S. Grand Strategy: Destroying ISIS and Al Qaeda, AQ and IS, “vie with each other for the leadership of the component of global Salafism.”

AQ became well known for fighting the Soviets when it invaded Afghanistan in 1979. Interestingly, the U.S. initially supported and funded AQ with about $20 billion, as a part of a proxy war to counter the Soviets during the Cold War. After the ouster of the Soviets from Afghanistan, AQ, under the leadership of Osama Bin Laden (OBL), turned against the United States, promoting the belief that the United States was the greatest threat to the Muslim world. As such, OBL prioritized the “far war,” successfully planning and executing terror attacks against U.S. embassies in Africa in 1998, the USS Cole in Yemen in 2000, and the 9/11 attack in the United States, among other attacks. These attacks also inspired dozens of affiliates across many countries and regions, creating multiple challenges to combat their terror threats.

For more than 20 years, U.S.-led counter-terrorism efforts devastated AQ operationally as well as many of its affiliates operating in central Asia and Africa. But, as the U.S. tired of war in Afghanistan, along with a Taliban resurgence and its ability to strike a deal with the U.S. Administration, the U.S. withdrew from Afghanistan in 2021. Some AQ affiliates have disbanded and all were weakened, but many remain in several countries and regions. Collectively, AQ presents a threat for the foreseeable future. The core Ideology of AQ and the U.S. as the strategic enemy of AQ has not changed. If left unchecked, AQ could re-emerge with a comparative strategic reach predating 9/11.

Turning to the IS movement, it was inspired by AQ and was initially affiliated with it, taking hold in Iraq after the U.S. invasion of Iraq in 2003. Eventually, IS split with AQ and became an even more aggressive terror group, to include killing fellow Sunni Muslims who were considered not as “pure” as its movement. With the U.S. withdrawal from Iraq in 2011 and a civil war in neighboring Syria, it created a security void that allowed IS to expand in size and geography. At its high point in 2015, IS controlled large portions of Iraq and Syria, with a population of about 12 million under its control and about one million people displaced. Beginning in 2018, the U.S. led a coalition called Operation Inherent Resolve to defeat IS. The operation was, and continues to be a success, with tens of thousands of IS fighters killed, its leaders targeted, and its territory largely recaptured. But like AQ, IS remains a threat, not only in the region, but it inspires attacks in the West, to include the United States. Though not ordered or controlled by IS, the most recent attack in the U.S. involved an IS-inspired individual that killed 15 in New Orleans on New Year's Day three months ago.

Shia VEOs:

In contrast, the Shia global leader is Iran, known for its involvement in and support of the “Shia Crescent” exhibited by Shia-based VEOs in the region spanning from northern Iran, through Iraq, Syria, and into Lebanon (via Lebanese Hezbollah), resulting in direct reach into Israel at its northern border. Iran openly states that it is a state sponsor of terrorism and that it seeks to eliminate Israel, and it uses proxies to help achieve this objective. Many leaders describe Iran’s threat to the region as more than a “Shia Crescent,” instead, they call it a “Shia Sphere” spanning not only north through Iraq, Syria, and Lebanon, but also south of Saudi Arabia through Yemen via the Houthis, into Gaza through Hamas and Palestinian Islamic Jihad (PIJ). The Oct. 7, 2023, Hamas attack into Southern Israel and the ensuing conflict is a clear manifestation of the Shia Sphere in action. Iran, the leader of the historic Persian Empire, still operates like the modern-day leader of a virtual Persian Empire through proxies that operate lethally, often with plausible deniability.

As a designated state sponsor of terrorism, Iran compensates for its lack of a formidable conventional ground force through its unconventional Qods Force (the foreign operations element of the Iranian Republican Guard Corps, or IRGC), which answers directly to Iran’s Supreme Leader Ayatollah Ali Khamenei and operates independent of Iran’s elected government. Arguably, the Qods Force is one of the most formidable special forces-like elements in the world. It conducts and enables operations and training unilaterally and operates mainly through partners and proxies in the region along with providing financial, political, and material support.

Since the Iran-Iraq War (1980 - 1988), Iran has demonstrated its ability to very effectively employ proxy forces to achieve its long game of a Shia Islamic Caliphate relative to its ability to effectively use its conventional forces and capabilities to deter and respond to Israeli, U.S., and international intervention. While Iran may not emerge as a nation with a large regular military force, its indirect approach through the IRGC, Qods Forces, and proxies appears to make up for conventional shortcomings.

Another proxy of Iran worth mentioning, is the Houthis in Yemon, a group of Zaydi Shias. The Houthis initiated attacks on shipping after Oct. 7, 2023, with about 70% of the normal traffic through the Red Sea diverting to other routes, adding stress to supply chains and increased costs. In response to these attacks, the U.S. formed a maritime coalition named Operation Prosperity Guardian to protect commercial shipping and freedom of navigation in the Gulf of Aden and the Red Sea. Since Oct 2023, the Houthis have launched 145 attacks against commercial vessels and 174 attacks against U.S. warships. The Houthis recently announced new renewed threats on shipping while they continued to attack U.S. warships, resulting in renewed U.S. strikes. In an interview with ABC, the White House national security adviser Mike Waltz said "… these were not kind of pinprick, back and forth -- what ultimately proved to be feckless attacks … this was an overwhelming response that actually targeted multiple Houthi leaders and took them out. And the difference here is, one, going after the Houthi leadership, and two, holding Iran responsible." Waltz later stated that U.S. Forces have “taken out key Houthi leadership, including their head missileer.”

Transnational Criminal Organizations (TCOs):

The term TCO is used by the White House, National Intelligence, and Federal law enforcement to refer to "groups, networks, and associated individuals who operate transnationally for the purpose of obtaining power, influence, or monetary or commercial gain, wholly or in part by illegal means." In the 2024 Annual Threat Assessment of the U.S. Intelligence Community, the Director of National Intelligence stated that TCOs "threaten U.S. and allied public health systems, exploit the international financial system, and degrade the safety and security of the United States and partner nations."

In contrast to VEOs that are primarily driven by religious ideology, TCOs, according to the FBI, have three goals: financial gain, control, and power. TCOs achieve these goals through a broad range of illegal activities such as trafficking of drugs, humans, organs, small and light weapons, cultural property, illegal mining, logging, fishing, wildlife trade operations; and running sophisticated counterfeiting, money laundering, and fraud networks.

TCOs are not only a threat to the U.S. and other free market nations' national security, but they also undermine governments and corporations, and threaten the very foundations of the global financial system. In the case of financial crimes, TCOs are a material threat. For instance, NASDAQ Verafin recently published a report highlighting the fact that over $3.1 trillion illicitly flows through the global financial system annually resulting in over $485 billion in fraud losses. The UN estimates money laundering alone represents up to 5% of the world's GDP.

According to the Director of National Intelligence, TCOs threaten U.S. interests by co-opting governments and weakening others. They forge alliances with corrupt government and business leaders to own and influence markets and trade, and their influence undermines competition in free and fair markets. TCOs are also known to provide funding and logistical support to terrorist organizations and are at the forefront of intellectual property theft and sophisticated cyber fraud. TCOs are businesses that employ violence, intimidation, and murder to ensure they keep their supply and distribution chains operating efficiently and effectively to respond to a market demand of over $100 billion per year in illegal drug demand in the United States alone. This demand is a humanitarian, social, political, and economic threat as it has resulted in the overdose of over 100,000 people a year, of which 70% can be attributed to fentanyl according to the CDC.

Every region in the world is adversely impacted by TCOs. Both Interpol and the FBI are working daily to combat them globally. Interpol is leading efforts for combating the increasing danger of TCOs like Ndrangheta, which has roots in Italy along with a network operating in more than 40 countries. Eastern European-based TCOs are heavily involved in complex cyber and healthcare fraud, financial crimes, identity theft, extortion, and drug and human trafficking throughout the world, including the Americas.

In the Americas, the FBI asserts that the threat TCOs pose to the U.S. and free market economies is expanding, and they identify the primary businesses for TOCs as sophisticated trafficking of drugs and people, and committing fraud. In many cases, TCOs are well-equipped and operate like a military. In Africa, another extremely dangerous TCO Interpol is tracking is Black Axe, a Nigerian TCO with over 30,000 members operating in dozens of countries, undermining development and political reforms and generating billions in revenue through global cyber scams.

In the Western hemisphere, the Cartel Jalisco Nueva Generacion (CJNG), which grew out of the Sinaloa Cartel, has become the most notorious. TCOs in Mexico are a primary conduit for international cybercrime, and drug, human, and weapons trafficking. It has its own financial and power interests and is also a connecting hub for other global TCOs that must traverse through Central and South American supply routes. Here is the link to a map from the National Consortium for the Study of Terrorism on the cartel routes in Mexico: https://www.start.umd.edu/tracking-cartels-infographic-series-major-cartel-operational-zones-mexico.

Eurasian TCOs are generally a hybrid, as they are both financially and politically motivated with strong connections to the Russian government. This hybrid motivation makes them fit the definitions of both TCOs and VEOs. In the Middle East, TCOs are often connected to VEOs like Hezbollah; and in Asia, many of the TCO groups have connections with the People's Republic of China with networks that have developed a significant presence in the Americas.
For businesses, TCOs are a threat usually thought of as outside their purview and left for governments to handle. However, TCOs are, in fact, businesses, and their markets compete with and include any business opportunities where they can achieve financial gain by breaking the law, exploiting weaknesses in the enforcement of the rule of law, and seams in public and private sector governance vulnerabilities.

What may seem like a pragmatic approach to compete and remain in business where TCOs are present is a real threat to free market nations that depend on fair trade practices. According to Reuters, it is not uncommon for multinational organizations to pay extortion payments to do business in foreign countries and participate in markets where they show a high presence. A study by the American Chamber of Commerce in Mexico found that 45% of companies doing business in Mexico have received demands for protection payments from cartels. The study also found that 12% of respondents stated that TOC had "taken partial control of the sales, distribution and/or pricing of their goods."

Economic concerns and due diligence to operate within the law:

Corporations spend a tremendous amount of time analyzing consumer trends, competitive responses, financial performance, regulation, technological developments and enterprise risks; however, most corporations do not focus on the strategic risk of Violent Extremists Organizations (VEOs) and Transnational Crime Organizations (TCOs). They rely on national security and global law enforcement institutions and tend to view mitigation of those risks out of their control. Yet VEOs and TCOs are areas of significant risk for businesses given their potential to disrupt operations, commit fraud, extortion, and intimidation against them or their customers. VEOs and TCOs present real tangible legal, financial, reputational, and physical risks to businesses.

The financial implications are material to the global economy, disruptive to free markets and businesses, and have significant unquantifiable impacts on humanity. Although VEOs and TCOs have different motives with similar actions posing threats to cybersecurity, supply chains, and currency flows, VEOs do not operate like organized businesses. TCOs, on the other hand, are generally structured like businesses with significant global reach, robust supply chains, financial networks, and quantifiable impacts. The U.S. Office of the Director of National Security (DNI) identified estimates for financial impact potentially totaling over $6 trillion spread across the following criminal activities: money laundering (up to $3.3 trillion – about 5% of world GDP);

bribery (approaching $1 trillion); narcotics trafficking ($1 trillion); pirated products ($500 billion); environmental crime (up to $40 billion); human trafficking: ($21 billion – with 2.4 million victims); credit card fraud (up to $12 billion); and firearms (up to $320 billion). Note that cybercrime, while not identified specifically in the DNI report, crosscuts all TCO illicit activities and is estimated by the U.S. government to be in the trillions annually.

There is a fine line between a designated VEO and TCO, which is important for businesses to understand. Under U.S. law, providing material support to terrorist organizations, VEOs can put businesses at risk of having their assets seized, being fined, and having criminal charges brought against leaders who knowingly engage with them. Similarly, if companies engage with TCOs, there can be legal sanctions, criminal charges if there is involvement in illegal activities, as well as damage to a company's reputation.

The threats from VEOs and TCOs are growing across the world with different regional areas focused on disparate types of crimes as reflected in the DNI report. It is important for businesses to address their potential exposures and formulate action plans to mitigate them.

Enterprise Risk Mitigation:

Given the macroeconomic impacts of the VEOs and TCOs, businesses should consider their direct and indirect exposures to this organized criminal activity. VEOs and TCOs are different and may require separate approaches in identifying, preventing, and mitigating risks; however, the mindset and frameworks for an organization are consistent for both.

Situational Analysis:

A strategic process is suggested for addressing VEOs and TCOs, starting with a strong awareness of the situation through senior leadership engagement. A risk assessment as part of an Enterprise Risk Management (ERM) exercise focused on VEOs and TCOs by region and function could provide a framework for understanding activities and the potential magnitude of risk for a company. Using internal management resources across operations, finance, technology, legal, human resources and security, along with external data or third parties could enhance such an assessment.

A company's enhanced risk assessment could help identify trends in activities that could be shared with law enforcement and peer groups also impacted by VEOs or TCOs. Such information sharing could help support national security, as well as protect the company and its industry by building stronger control systems.

All industry sectors have potential risk and should have an awareness of the exposures and disclosure regulations to help them know their customers, vendors, business partners, funding sources, and potential acquisition or divestiture counterparties. This mindset should be incorporated into customer relationships and due diligence activities.

While financial and cyber risks have the highest potential magnitude, intellectual property theft, supply chain disruptions via piracy, and free market disruptions through manipulation are other areas where they could have significant exposures.

The largest threat identified by DNI is money laundering. Financial institutions across the globe, and especially in the U.S., are one of the most heavily regulated industries requiring large compliance programs focusing on transparency including Know Your Customer (KYC) rules regarding customer identification and ongoing monitoring. The U.S. government provides tools through the Office of Foreign Assets Control (OFAC), which provides automated sanctions lists for businesses to compare against known potential criminal entities. There are many U.S. regulations for the financial service institutions that require timely reporting of transactions (within 10 days) that support law enforcement to track patterns of currency movements that could help control terrorist and criminal organizations' activities.

Likely, many of the risks associated with these criminal activities already have internal controls, compliance activities, and staff assigned to monitor. For example, business cybersecurity activities are likely already providing awareness and controls over access, data security and encryption, data storage, intellectual property, and ransomware attacks. Yet, an assessment might enable the identification of existing gaps or future opportunities where threats may not exist.

VEO and TCO Economic Risk Areas:

The primary implication is that businesses have responsibilities, both legal and fiduciary, to understand how their business model eco-systems may be impacted by VEO and TCO activities.The ecosystem for a business includes people, processes, and systems.
People: business stakeholders include employees, investors, suppliers, and outsource vendors; businesses are responsible for knowing about them and protecting them both physically and reputationally.

Employees: employee awareness, pressures inside and outside the work environment, and infiltration that leads to insider threats pose significant risk. Thorough background checks, proper training to build awareness and understanding of compliance requirements, safe working conditions to provide safety and security across the globe, and logistical security to protect privacy.

Customers: data privacy, sanction compliance, banking, and treasury compliance.
Investors: investment risk, transactional risks associated with accepting investment from sanctioned parties, and foreign direct investments without sufficient due diligence.
Third-Party Suppliers, Vendors, and Outsources: transparency of activities, funding sources, background checks, and data security.

Process: business processes include all business activities throughout a business' value chain. Supply chain management visibility and communication, product development, Intellectual Property protection, asset management and theft, cybersecurity, human resource processes, internal control systems, and financial and legal requirements and disclosures.

Systems: business systems include all information technology systems, data storage, transmissions and interfaces with third-party vendors including financial institutions—physical and logical security of IT infrastructure with a focus on cybersecurity and redundancy.

Governance: businesses operate within various legal authorities and regulatory environments. They are often at the forefront of where TCOs operate as they are physically in the markets. However, they do not have the authority to enforce legal and fair trade, which is totally in the purview of governments. Governments, on the other hand, are not in the business of developing supply chains or providing goods and services to free markets. They are there to enforce the laws and policies that enable markets to be as fair and free as possible. It is incumbent on businesses and governments to increase collaboration and accountability for identifying VEO and TCO impacts and suspicious activity to ensure markets can operate efficiently, effectively, and legally.

Take Aways:

- Risks continue to increase and become more sophisticated with technological advancements.
- Legal, financial, operational, reputational, and physical risk can be material and strategically relevant.
- A strategic approach is needed to identify, evaluate, mitigate, and monitor risk.
- Risk frameworks should include robust assessments and communication processes and controls that ensure higher levels of collaboration with law enforcement and the intelligence community.