FiveBy

ADVISORY

Strategic Corruption: Be Ready to Act

In June, 2021, the Biden administration issued a memorandum establishing the fight against corruption and kleptocracy as a core national security interest. In December, the White House issued the "United States Strategy on Countering Corruption" that aims to enhance the nation's "capacity to identify, track, and disrupt illicit finance" as it pertains to kleptocracy and corruption. The White House specifically flags strategic corruption as a national security threat, noting that foreign adversaries weaponize corrupt practices as part of their foreign policy to advance their geopolitical goals. The Financial Crimes Enforcement Network (FinCEN) almost certainly will implement additional regulations and issue guidance to help US firms and financial institutions identify and block corrupt actors' access to the US dollar and make tackling strategic corruption a priority this year. US firms and financial institutions should stay ahead of possible regulatory changes and reassess their risk appetite, lines of business, and possible vulnerabilities.

What is Strategic Corruption?

Corruption largely means the abuse of public office for personal gain, and strategic corruption is a particular subset of that general definition in which adversarial governments use either government or proxy actors to further their foreign policy objectives. Strategic corruption does not seek to gain personal or business advantages—although personal or business gain are often a benefit—but rather helps the corrupt government shape its foreign policy outcomes, making it a national security concern for the United States.

In a recent address to the American Bankers Association, FinCEN acting director Him Das noted the proliferation of strategic corruption aimed at weakening US institutions. Strategic corruption can include various tactics that can be used to influence foreign countries' governments, democratic institutions, and foreign policies.

Buying political influence. Oligarchs—especially from Russia and Ukraine—are making real estate and other large asset purchases to launder money through US and other western financial systems and influence politicians. Corrupt regimes also exploit state-owned companies to influence foreign politics. The Kremlin uses its energy and defense sectors and private business surrogates to launder money, funnel it to its preferred candidates, finance political campaigns, and influence foreign leaders.

- To advance Russia's energy policy in Europe, the Kremlin gave former German Chancellor Gerhard Schröder "a highly-paid board position" on Gazprom's Nord Stream project, which has sparked disputes in the EU and in Germany about European energy security. Russia also gave former Austrian Foreign Minister Karin Kneissl a position with its state-owned oil company, Rosneft, and former French Prime Minister Francois Fillon a position with energy company Zarubezhneft, coopting elites in those countries to further Russia's geopolitical goals.

- In November 2017, US authorities arrested Patrick Ho, an executive from Chinese energy conglomerate CEFC China Energy, on bribery and money laundering charges after he paid off African leaders to open oil and gas markets on the continent to China, "arranged for illicit arms sales to Libya and Qatar," and "offered to help Iran move sanctioned money out of China." A CNN report in 2018 showed that CEFC China Energy had aligned itself closely with the Chinese government, and Beijing took over CEFC after Ho's arrest.

INFO@FIVEBY.COM

- To counter corrupt actors' efforts to access the US financial system, US regulators could increase reporting obligations for real estate cash transactions, enhance corporate transparency requirements, and increase regulatory requirements for professional services, such as attorneys and other gatekeeper professions that facilitate corrupt actors' entry into US markets.

Military corruption. Transparency International assessed that in 2021, more than 60 percent of the countries in the world were at a high to critical risk of defense sector corruption, which can undermine military peacekeeping and homeland defense operations, as well as divert military materiel to corrupt or adversarial countries and terrorist and criminal groups. The White House countercorruption strategy includes measures to address corruption in military structures, including using newly created anticorruption task forces at the Commerce Department and USAID to press risky countries for accountability.

- Russian troops faced little resistance from Ukrainian forces when they invaded Crimea in 2014, facing a Ukrainian military weakened by decades underfunding and outdated equipment, while more modern and effective equipment was sold by corrupt military officers to nations such as China and Pakistan for cash.

- Efforts to clamp down on strategic corruption will significantly impact military contractors, who will almost certainly need sound anticorruption programs to stay ahead of possible regulatory changes. The Strategy mentions strengthening analysis of corruption risks in security cooperation and military operations and planning by developing training, assessing political will of military partners, and conducting more frequent security cooperation evaluations to ensure transparency and accountability.

Cybercrime. In the first half of 2021, FinCEN received 30 percent more ransomware-related suspicious activity reports than in the entire previous year. In late January, the US Department of Homeland Security warned that Kremlin-backed hackers could soon target critical US infrastructure, such as utility providers and banks. The White House countercorruption strategy notes that the US government will continue assessing how digital assets and cybercrime support corrupt actors and how corrupt regimes use ransomware and other illicit cyber activities to further their foreign policy goals. The efforts to counter the threat will almost certainly include additional designations against digital wallets linked to malign actors and increased cooperation between law enforcement and private-sector entities to identify, track, and recover ransom payments and take down malign actors.

- Ransomware operations are dominated by Russian-speaking cyber actors, and Russian intelligence agencies turn a blind eye to, protect, and sometimes support these criminals, as long as they do not target Russian assets and occasionally perform tasks for the government. Possible government tasks include targeting adversaries' financial institutions and critical infrastructure as a form of hybrid warfare.

- FinCEN and other government agencies will play a key role in the battle against ransomware and state-linked cyber actors by issuing advisories and working with law enforcement to recover funds. The US government will almost certainly also focus on mixing services, virtual currency exchanges, and other operations that help malign actors conceal transfers of cybercrime proceeds. Treasury has an array of cyber-focused sanctions tools and an expansive executive order targeting Russia's malign activities at its disposal to mitigate the risk of malicious cyber-attacks linked to state actors.

Staying Ahead of the Curve

US firms must be forward leaning in their efforts to examine their compliance programs and reassess their risk appetites regarding corruption. Strategic corruption red flags include jurisdictional risks, lack of transparency, involvement of politically exposed persons in financial transactions, and other indicators.

Russia and China are known for weaponizing corruption to achieve their geopolitical goals, but other countries, such as Turkey and Azerbaijan, also use this strategy. Turkey's state-owned Halkbank is accused of helping Iran evade US sanctions, and several attorneys with links to the US government were involved in efforts to free a Turkish businessman connected to the sanctions-evasion conspiracy. Azerbaijan and other post-Soviet states like Kazakhstan have coopted elites, creating kleptocratic networks to further foreign and domestic policy goals.

Jurisdictions labelled as being of primary money laundering concern by FinCEN under Patriot Act Section 311, such as Iran and North Korea, or greylisted for AML/CFT strategic deficiencies by FATF also tend to weaponize corruption as a tool to further their geostrategic goals.

On December 7, 2021, FinCEN issued a proposed Beneficial Ownership Reporting Rule, soliciting comments from stakeholders who would be required to file Beneficial Ownership Information (BOI) reports. US firms and financial institutions should be particularly cautious about transacting or working with entities whose ownership and control is hidden behind a web of shell or front companies, as well as those located in jurisdictions with lax transparency requirements that do not require the identification of ultimate beneficial owners.

Although the involvement of a politically exposed person (PEP) in a business transaction or a company structure does not, in and of itself, indicate the presence of strategic corruption, PEP status warrants additional scrutiny. FiveBy advises that enhanced due diligence is particularly important when the PEP is working in vulnerable industries, such as real estate, energy, defense, or IT, or in risky jurisdictions, or has an unexplained amount of wealth. Companies engaged in these sectors should reassess their risk programs, possibly perform transaction monitoring, track changes in employment for clients—especially in risky jurisdictions or who raise other red flags—and should keep abreast of possible upcoming regulatory changes mandated by the Corporate Transparency Act, given the Biden administration's commitment to treating corruption as a national security concern.