INTELLIGENCE AND CORRUPTION

Andrew Dalip, Jr.
LL.B (Hons.), L.E.C., M.Sc. (Dist.), C.A.M.S., C.G.S.S.

The Journal of Intelligence, Conflict, and Warfare is pleased to publish the following thought piece from one of our esteemed Speakers from the 2020 West Coast Security Conference. The author, Mr. Dalip, is a lawyer working in the financial crime and corruption sphere. From 2015 to 2018, Mr. Dalip was a chairman at the Steering Group Planning Committee for the Caribbean Financial Action Task Force (CFATF); and from 2014 to 2018, he was a special legal advisor to the Ministry of Attorney General Trinidad and Tobago.

Keywords: corruption, intelligence, financial intelligence, FATF, money laundering, sanctions.

Abstract

The intersection between corruption and intelligence is gaining increased focus. Foreign intelligence services have an anti-corruption role at the strategic level through Intelligence Risk Assessments and at the operational level during post-conflict operations. Intelligence assessments of the effectiveness of non-kinetic tools on target countries also guide implementation and policy changes.

The roles of security intelligence and foreign intelligence services are, however, no longer always discrete, particularly in the context of non-state actors. Foreign intelligence services would benefit from the skill sets of security intelligence agencies in detecting corruption related predicate offences, both in performing their core roles and supporting law enforcement operations. This includes the use of financial intelligence as well as other key open source intelligence resulting from anti-money laundering frameworks, the development of which has been driven globally by the Financial Action Task Force. In performing these roles, intelligence agencies must also be mindful of their own vulnerability to corruption.

Intelligence and Corruption

2020 was a cataclysmic year for the global community, exponentially increasing the demands placed on governments, impacting on the delivery of many key public services. As household revenues evaporated and entire sectors of the economy collapsed, dependence on the state increased bringing shortfalls in service delivery into focus. This has thrown a spotlight on corruption as people seek explanations for why their governments were not better prepared.

Even before the COVID-19 pandemic, corruption has been a significant driver of social unrest in scenarios ranging from the Arab Spring uprisings, where many protesters were reacting to deeply entrenched corruption in the region, to the Ukrainian revolution, which was partially in response to corruption by Viktor Yanukovych's government (Transparency International Defence & Security [TIDS], 2019; Chayes, 2014a). Corruption erodes public trust and confidence in the organs of the state. When combined with other factors including economic inequality and ethnic and religious tension, the social fabric begins to unravel (Chayes, 2014b). This paves the way for states to lose control of territory, whether to criminal gangs on a localized scale or terrorist organizations over vast regions.

A country may suffer critical structural impacts, as corruption in the public and private sectors can result in severe economic distortions (Ahmad et al., 2012; Chayes, 2014b). These can lead to governments intentionally or unintentionally prioritizing unprofitable sectors while leaving more structurally important industries to suffer. The cascading effects both create an environment of instability and ultimately increase the suffering of the most vulnerable in society (Chayes, 2014b).

Corruption not only presents security risks within states but can also impact on international relations. The spoils of corruption are spirited away from developing countries to be enjoyed in developed states. This illicit capital flight widens the wealth gap between the first and third worlds (Transparency International [TI], 2020) all of which feeds particularly into the narratives of terrorist organizations (Chayes, 2014b).

While corruption has now also become an area of focus for the military, it has long been on the agenda of law enforcement agencies. In fact, both the military and law enforcement operate in the domains of the intelligence community, albeit often different services, each with a traditionally distinct mandate.

Corruption in Context and Corruption as Context

Any study of the different ways in which corruption and intelligence intersect must be premised on an understanding of key elements of the issue of corruption. It must be recognized that in some circumstances, corruption is so deeply entrenched that it is no longer a perversion of the system; it is the system. Gaps or inefficiencies in service delivery may not be a consequence of corruption, but

instead an integral feature critical to sustaining the system itself, creating a level of dependency that allows kleptocrats to exploit the public (Chayes, 2014a).

This can take place in a hierarchical way, with corruption pervading the entire governmental structure and centralization of control of exploitation. This may involve attempts to legitimize otherwise corrupt behavior, through control of the legislature and even appointments to the judiciary. In other cases, it may be more diffused and driven from the bottom up with corrupt actors in key institutions (e.g. customs and tax authorities) who may purchase the support or indifference of politicians to maintain the status quo.

Know the Terrain

Policymakers, aid agencies, private sector investors, the military, and intelligence agencies must therefore understand corruption as a feature of the terrain they wish to operate in, and as such, an important part of the intelligence picture. Failure to do this can result in a host of challenges, whether actors are engaged in anti-terrorism or counter-insurgency missions or Phase IV or V post-conflict operations. These can include:

- Enabling corrupt governments, exacerbating the security threat;
- Engendering hatred of that country's population towards our country as we will be seen as endorsing their corrupt government;
- Engendering hatred in our own country because we support corrupt regimes; and
- Compromising our ability to achieve our ultimate strategic objective in that country (Chayes, 2014b; Joint and Coalition Operational Analysis [JCOA], 2014).

The Case of Afghanistan

The mission in Afghanistan over the last 2 decades provides a good case study of these challenges and has been rigorously examined by several institutions including JCOA (2014), TI (2014) and TIDS (2018).

The US and its allies have had forces deployed in Afghanistan since 2001, commencing Operation Enduring Freedom in response to the 9/11 attacks. The stated intent was to disrupt the use of Afghanistan as a terrorist base of operations and specifically to attack the military capability of the Taliban. In 2002, the International Security Assistance Force (ISAF) entered the theatre pursuant to a

UN Security council mandate. This multi-national force ultimately morphed into a NATO operation in 2003 and expanded beyond its initial scope of securing Kabul, to ultimately having a presence throughout Afghanistan. The ISAF was wound down in December 2014 and was succeeded by NATO's Resolute Support Mission, which is aimed at training and supporting the Afghan National Defence and Security Forces. Operation Enduring Freedom also officially came to an end simultaneously with ISAF operations and was succeeded by Operation Freedom's Sentinel, which covers both US operations as part of Resolute Support and counter-terrorism missions.

Corruption was not a part of the mandate for perhaps the first decade of this deployment, with the focus being on tactical objectives. This, however, changed by 2012, at least at the policy level, as corruption became a part of the NATO Operational Plan, with the ISAF Commander being tasked to 'neutralize corruption and organized crime.' This new mandate, perhaps, reflected renewed international attention on corruption, particularly with the United Nations itself still reeling from the Iraq "oil-for-food" corruption scandal (McMahon, 2006).

However, even the new tasking still overlooked the impact of corruption on achieving the overall strategic objectives of these missions, particularly to stabilize the country and enable civil authorities. The effect of the US and ISAF missions was in some respects exactly the opposite, with these operations unintentionally facilitating the deepening of corrupt practices. The sheer quantum of money and resources poured into a country battered by decades of conflict provided unbridled opportunity for corruption. On average, the US alone has injected close to US$8 billion per year in assistance to Afghanistan, far outstripping the institutional capacity of the country. Little capacity for oversight fed the desire of the unscrupulous and classic mechanisms for diversion of funds, and the abuse of state institutions flourished. Resources intended for the rebuilding of the country ultimately began finding their way into the hands of the insurgency.

Afghanistan is not unique as an example of corruption ultimately compromising security. UN reports, for example, point to law enforcement officers in Kenya often accepting bribes to let Al-Shabaab operatives across the border from Somalia with arms to support terrorist activities, including for the Westgate Attack in 2013 (Chayes, 2014b).

Local Partners

Foreign forces often partner with local allies to pursue core mission objectives including counter-terrorism and counter-insurgency. In Afghanistan, however, this shifted the balance of power on the ground, acting as an endorsement of those local actors by foreign militaries which were the new foundation of authority in the country. Thus, in addition to directly obtaining foreign financing and materiel intended to support the war effort, together with contracts to supply foreign forces with everything from construction material to petrol, the local powerbase of these *preferiti* grew, giving them further leverage over the local population. These local powerbrokers were placed in a unique position nationally, and essentially marketed the backing of foreign powers to build their empires. It was, however, cyclical as they ultimately monopolized mission-critical sectors, such as construction, jacking up prices including for goods and services to US and NATO forces.

Often, these local partners also became the foreign force's primary source of intelligence on the ground, with the direct and indirect financial reward creating a perverse incentive to continue the flow of such intelligence. This ultimately corrupted the intelligence gathering process with much of it not actually being credible, thus compromising the US and NATO mission objectives (TIDS, 2018).

The Enemy Within

Intelligence gathering and information security go hand in hand, and corruption has long been both an ally and an enemy of intelligence services. Susceptibility to bribes or having corruption skeletons in the closet makes government officials vulnerable to exploitation by intelligence services. Conversely, intelligence officers have the same financial obligations as the rest of society and are sometimes equally or even more vulnerable to exploitation by foreign agents.

There are several names that fall into this category including Aldrich Ames of the United States Central Intelligence Agency (CIA) and Robert Hanssen of the United States Federal Bureau of Investigations (FBI) (Defense Personnel Security Research Center, 2004). These incidents can have devastating consequences for morale within the agency and severely erode public trust and confidence in the intelligence service as a whole. Canada's intelligence community is also not immune to such vulnerability, as exemplified by the case of Jeffrey Delisle (Nova Scotia Department of Justice Correctional Services, 2012). Debt and financial obligations reportedly factored in the cases of all three of these officers: Ames had alimony payments; Hanssen struggled to provide for

a large family and had incurred hundreds of thousands of dollars in debt; and when Delisle began leaking information in 2007, he had incurred significant credit card debt, which had also been a factor in his filing for bankruptcy 10 years earlier.

The roots of motive may sometimes extend far deeper than financial independence. Ames' desire for money, for example, was reported to be in part due to the lifestyle demands of his new wife. Hanssen used a significant portion of his money to maintain his mistress, while Delisle claimed that his trigger for offering to sell secrets to Russia was discovering his wife had been unfaithful. Understanding these catalysts, therefore, can help intelligence agencies establish internal controls for prevention and detection of corruption by their personnel.

Officers involved in security intelligence[1] (including criminal intelligence gathering) can also be susceptible to corruption. Hanssen, in fact, worked for the FBI whose mandate is law enforcement and domestic intelligence. Corrupt intelligence officers can, of course, funnel information to drug lords and criminal gangs for a price, and, conversely, feed misinformation to their agencies to cover the tracks of their criminal allies. United States Drug Enforcement Administration (DEA) Special Agent Fernando Gomez was indicted for his participation in a conspiracy to distribute cocaine as well as possession of firearms, and aiding and abetting the possession of firearms in furtherance of that drug conspiracy with a Puerto Rican drug cartel, *La Organizacion de Narcotraficantes Unidos* (United States Attorney's Office [USAO], 2018).

The lines between security intelligence and foreign intelligence have become increasingly blurred, particularly in the context of the wars on drugs and terror. Both cases, deal largely with non-state actors and have traditionally been law enforcement issues. The illegal narcotics trade is a transnational organized criminal industry on a scale that has been recognized as threatening the national security of North American and European countries since at least the 1980's. Military resources, including military intelligence assets, have been sunk into this fight on a mammoth scale (Best, 2010). The drug trade is a multi-billion dollar industry, adding to the risk of corruption of military and intelligence officers and their human intelligence assets, thereby polluting the intelligence gathering and analytical processes. The case against Fernando Gomez alleged

[1] For the purpose of this paper, "Security Intelligence Service: refers to intelligence agencies whose jurisdiction covers domestic threats while the mandate of the "Foreign Intelligence Service" is information relating to the political, economic and military activities of foreign states.

that he joined the DEA specifically to serve as a mole for the cartel (USAO, 2018).

Future Risks

One of the key roles of the intelligence community is to prepare intelligence risk assessments, i.e., future scanning for risks over the medium to long term. These risks can come from both enemies and allies. For example, with the end of the Cold War and the dismantling of the Soviet military apparatus, an estimated 2.5 million tons of conventional munitions were left in the Ukraine, far beyond the capacity of that country to absorb, safely dispose of, or even properly secure. Over time, much of that materiel (ranging from assault rifles to surface-to-air missiles) found its way into conflicts in Africa, Asia, and the Middle East with little to no accountability for its movement. The risk is not only that such items find their way into the hands of foreign militaries and combatants in civil wars, but also terrorist organizations (Chivers, 2005).

The dismantling of the Soviet Union also raised the specter of nuclear materials and other WMDs falling into the hands of rogue nations and terrorists. There were reports of ex-Soviet scientists, military personnel, and intelligence officers attempting to sell fissile material, as well as suitcase sized nuclear devices being unaccounted for (Lee, 2001). On the demand side of the equation, both rogue states and terrorist organizations alike have attempted to acquire WMD material and technology. Corruption can feed the proliferation of conventional weapons and WMDs not only through the supply of materiel, but also through financing. Saddam Hussein, for example, used money siphoned from the "oil-for-food" programme to build a missile system exceeding the range limits imposed by the UN after the end of the First Gulf War (Otterman, 2005).

It is, therefore, important for intelligence risk assessments to identify these possibilities, even where non-kinetic options, such as diplomatic pressure or economic and trade strategy, are the chosen means of achieving political or foreign policy objectives.

Friend or Foe?

Today's allies can also be tomorrow's enemies, especially if corrupt or potentially corrupt actors are chosen as preferred partners. The risks include military assets and technology falling into the hands of hostile states. For example, Venezuela was once a close ally of the United States and even remained a major trading partner despite political tension following the rise of

Hugo Chavez as President in 1998. The relationship has deteriorated further since Nicolás Maduro assumed the Presidency after Chavez's death in 2013. The Maduro administration is regarded by the US and many Western and Latin American countries as patently corrupt, abusing state assets such as the national oil company PDVSA. In 2020, the United States Department of Justice preferred criminal charges against Maduro and fourteen other Venezuelan officials for allegedly being involved in narcotrafficking, narco-terrorism, and money laundering (United States Department of Justice [USDOJ], 2020).

By 2005, Chavez announced he was ceasing cooperation between the Venezuelan and the US militaries. The US, in turn, has prohibited the sale of defense articles and services to Venezuela since 2006, citing lack of cooperation on anti-terrorism efforts (Sullivan, 2009). Venezuela, however, has a fleet of US made F16s acquired in 1983, and though a few have been lost to crashes, the majority remain in service. While the contract for supply of the F-16s prohibits their resale without US consent, Venezuela undoubtedly rattled a few cages in the 2000's by proposing to sell them to Iran (Military Watch Magazine, 2019). Now, with the relationship between Maduro and the US being at a continuing low, and Venezuela dealing with an economic crisis and a huge debt to Russia, coupled with strong defence ties to that country, the specter of a possible transfer of the F-16s to Russia[2] has been raised in some quarters. While this has been dismissed by some as simply grandstanding, it still reinforces the importance of keeping the medium to long term strategic picture in mind when dealing with the transfer of weapons, technology, and even training.

Economic Warfare and Corruption as Statecraft

The vulnerability of individuals or a country's government to corruption presents opportunities for exploitation, not only by criminal enterprises, but also foreign states. TIDS (2019, p.1) describes this as "corruption as statecraft," citing examples of corruption as a foreign policy tool either by itself or in conjunction with other measures, such as disinformation and cyber-attacks. TIDS (2019, p. 3) cites Moscow allegedly leveraging Ukraine's dependency on gas imports

[2] Such technology grabbing is not a one-way street. In the Cold War both sides tried and succeeded in obtaining the other's technology for evaluation. In 1977 under Anwar Sadat, Egypt realigned itself on the international stage and provided the US with MiG 23s for evaluation, breaching one of the conditionalities of supplying the fighters to Egypt. The MiG 23 was a relatively new 3rd Generation fighter at the time capable of outperforming the F4s flown by Israel. The US Air Force 4477th Test Evaluation Squadron flew these and other acquired Soviet Aircraft to familiarize US fighter pilots with their performance and tactics.

from Russia to influence Ukrainian domestic and foreign policy. TIDS (2019, p. 3-6) also suggests that over the last two decades, this has been achieved through a combination of pressure and bribery of key players within the Ukrainian energy sector.

Von Clausewitz (1832) said "war is the continuation of policy by other means" (p.18). The theater and method of warfare are not, however, cast in stone. Belligerent states have taken steps short of actual armed conflict for centuries, either as an alternative or as a precursor to kinetic solutions. As far back as 432 BC, the Athenian Empire issued the Megarian Decree. This banned Megarians from harbors and marketplaces throughout the Athenian Empire, putting a stranglehold on Megara's economy. While there is some academic debate as to the motive for the decree, the Peloponnesian War began soon after in the year 431 BC.

Economic warfare as a foreign policy tool is, therefore, not a new development but has continued to be used up to modern times. The Cold War was a battle of ideologies pitting the political and economic philosophies of socialism and capitalism against each other. The Reagan administration's strategy included economically isolating the USSR from the rest of the world (Dobson, 2005). Now, decades after the fall of the Iron Curtain, a trade war between the US and China has emerged. The US has long accused Russia and China of economic espionage, stealing secrets from the western military industrial complex, and ultimately threatening national security. Industrial espionage from China in particular, allegedly takes place on a scale that can tip national economies. The FBI estimates that economic espionage costs the US approximately US$500 Billion per year (Gates, 2020), while the Commission on the Theft of American Intellectual Property (2017) puts the cost of trade-secret theft at between 1 – 3% of GDP or between $180 and 540 billion. In the UK, estimates suggest that around £1.2 billion is lost through industrial espionage and intellectual property theft in the aerospace and defence sectors alone (Cabinet Office & Detica, 2011).

The Response: Detection, Prosecution and Interdiction

Faisceau d'indices[3]

Whether countries aim to prosecute or sanction corrupt actors or to identify individuals who are vulnerable to being exploited, the starting point is

[3] In the present context, "*faisceau d'indices*" refers to a range of indicators that point to the legal elements of corruption related offences possibly being satisfied.

intelligence that points towards the legal elements of an applicable corruption-related offence being satisfied. While human intelligence (HUMINT) continues to play a critical role in detecting corruption, open source intelligence (OSINT) is also carving out an increasing space in intelligence gathering in this arena. There are daily examples of its use by both law enforcement and compliance officers within financial institutions (FIs), and designated non-financial businesses and persons (DNFBPs) around the world[4]. Individuals and companies post a great deal of exploitable information on the internet and in journals. This can help to identify ripe target organizations, as well as vulnerable human assets within those organizations.

Financial Intelligence

One key form of intelligence relating to corruption is financial intelligence, which forms the backbone of AML/CFT/CFP[5] regimes. The fight against corruption has been one of the main drivers behind the development of international anti-money laundering standards by organizations, such as the Financial Action Task Force (FATF). The FATF Recommendations, which have been accepted by 202 countries and supranational bodies, require countries to establish laws or other enforceable means, tackling money laundering and the underlying predicate offences together with allocating the resources to implement those laws and demonstrating that they are being used (FATF, 2019). This covers the detection, tracing, confiscation, and return where appropriate of corruption proceeds, as well as promoting international cooperation in all of these areas.

FATF Recommendation 36, for example, requires countries to become part of and implement fully into the United Nations Convention against Corruption, 2003. The FATF has driven the development of laws, policies, and systems to tackle money laundering and predicate offences, including corruption related crimes such as bribery, theft, and organized criminal activity. The establishment of national Financial Intelligence Units (FIUs) and integrating them with the global network of FIUs through the Egmont Group[6] is a cornerstone of these systems. FIUs, in turn, rely on banks and other FIs as well as DNFBPs who deal

[4] For definitions of FI and DNFBP see, FATF Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems [FATF Methodology] (2020b)
[5] Anti-money laundering, combatting the financing of terrorism and combatting the financing of proliferation of weapons of mass destruction.
[6] The Egmont Group of Financial Intelligence Units.

in high value commodities and assets (e.g., real estate agents and jewelers) and intermediaries (e.g., lawyers and trust and company service providers) as primary sources of information. These FIs and DNFBPs are obliged by law to exercise appropriate levels of due diligence with respect to their regular and occasional customers based on the risk posed. Such customer due diligence (CDD) takes into account factors, such as the background and nature of the customer (e.g., foreign or domestic politically exposed persons, sanctioned individuals or relatives, or companies involved in import/export); the financial product or service involved (e.g., cross-border wire transfers); and relevant jurisdictions (e.g., through nationality, source, transit or destination of imported/exported goods or funds).

FIs and DNFBPs are required to develop and implement a risk-based CDD system and a sanctions due diligence system, allowing them to detect suspicious transactions in relation to the ML and sanctions violations respectively. Due diligence systems build on the FI or DNFBP's industry experience together with knowledge of their customers acquired through relationship management, to recognize behavior or activities which are atypical. This includes transactions relating to corruption and can involve politically exposed persons (PEPs), mid-level government officials, such as customs officers, and even military and intelligence officers.

Underlying this is also a requirement for these institutions to keep adequate and up-to-date records of their customers, transactions, risk assessments, and reporting. These can all play an important role in analyzing patterns of transactions to determine if any of them is unusual, serving as evidence in the event of a prosecution or other legal intervention. If a transaction is flagged as suspicious by the FI or DNFBP, then the institution has a legal obligation to file a suspicious transaction report (STR) with the FIU within a specific timeframe, providing adequate details of the transaction including what was sufficiently out of the ordinary to make it suspicious. The FI or DNFBP, however, also has to take steps to prevent the "suspect" from knowing an STR has been filed to avoid tipping them off.

The FIU will then examine the STR, requesting other information from the reporting entity as necessary. This information will be analyzed in the context of known or emerging typologies for corruption-related money laundering, other STRs, and information gained from other FIs and DNFBPs, as well as OSINT to distill all this information into financial intelligence. While some FIUs are hybrid and fulfill a dual intelligence/investigative role, many are characterized as

administrative FIUs. These are restricted to compliance functions and collection, analysis, and dissemination of financial intelligence to law enforcement agencies. Thus, where the intelligence suggests that a predicate offence such as a corruption-related crime has taken place or been attempted, the FIU prepares an intelligence report and sends it to the relevant law enforcement agency (LEA) for investigation (e.g., the police, revenue service, customs, and excise or agencies responsible for sanctions enforcement).

One of the strengths of this system is that it gives the FIU access to the eyes and ears of the FIs and DNFBPs. FIs, in particular, often have a significant extraterritorial reach especially where they are multi-national institutions. FIs, in fact, have an obligation under FATF Recommendation 18 to implement group-wide information sharing programmes for AML/CFT/CFP purposes. Some of these truly global players, for example, can develop link charts and identify typologies faster than FIUs or other agencies, simply because they have ready access to information provided to them directly by their clients. If some information is missing, they can even ask the client to fill in the gaps in order to comply with their legal due diligence requirements.

The FATF Recommendations also catalyzes the collection of other key information. This ranges from information related to:

- how money is moved (such as ensuring information on the parties involved in wire transfers of US$1,000 or more is provided to all FIs along the transfer chain), as well as rules governing correspondent banking relationships and controls on the movement of cash and bearer negotiable instruments;
- “fit and proper” testing of controllers of entities at particular risk of abuse for ML of corruption proceeds (such as banks and casinos); and
- basic and beneficial ownership information for companies and trusts, which are structures often used to obscure transactions. These legal persons and arrangements can feature in corruption and ML in many ways, including the use of shell companies and private investment companies set up in offshore jurisdictions to hold property, front companies to launder money, and companies purchased as the end product of ML at the integration stage.

Financial intelligence can ultimately lead to a financial investigation, and the FATF Recommendations require countries to have laws and systems in place to

provide for the investigation of these predicate offences. This includes ensuring LEAs have legal authority to use special investigative techniques long used by the intelligence community, including interception of communications, undercover operations, and accessing computer systems.

Taking the Profit out of Corruption

Countries are not only required by the FATF Recommendations to criminalize ML and predicate offences related to corruption,[7] but also to establish mechanisms to take the profit out of these crimes[8]. Conviction-based asset forfeiture has long been a feature of AML systems. While, as the name implies, this is predicated on a successful prosecution, there is often a wide gap between intelligence and actionable criminal evidence. Therefore, globally, there has been a greater shift towards non-conviction based asset forfeiture and "explain your wealth" legislation. This applies a considerably lower evidential standard (more closely approximating to intelligence) and often shifts the burden to the suspect to prove the legitimacy of the source of his wealth. Therefore, if *bona fides* cannot be proved, both money and property are forfeited to the state.

Domestic and International Cooperation

FATF Recommendations 37 – 40 also stress the importance of mechanisms for international cooperation for sharing intelligence, procuring evidence, extradition, and asset seizure, including the sharing of seized assets when joint international operations are successful. This, therefore, provides opportunities for intelligence-led international operations, particularly as the FATF requires countries to go beyond enacting legislation and must demonstrate these laws are being effectively implemented. The experience of countries implementing the FATF Recommendations, also reinforces the importance of the taskforce approach in tackling corruption, bringing all key LEAs and intelligence agencies around the table to short-circuit information sharing for intelligence and investigative purposes.

There are success stories of FIs being directly integrated into this network, such as the UK's Joint Money-Laundering Intelligence Task Force (JMLIT) and Australia's AUSTRAC Fintel Alliance. Such public-private cooperation is not only critical to providing intelligence agencies with timely access to information from FIs and DNFBPs. Improving the quality of information provided by these

[7] Recommendation 3.
[8] Recommendation 4.

institutions is dependent on feedback provided by LEAs and the intelligence community through FIUs. Similarly, LEAs and the intelligence community furnishing the sector with updated typologies of corrupt practices can assist FIs and DNFBPs to better detect corrupt actors.

OSINT Emanating from the FATF process

These FATF-driven processes also generate important OSINT for domestic and international LEAs and intelligence agencies. FATF Recommendation 1 requires countries to assess their ML, terrorism financing, and (most recently), proliferation sanctions risks (FATF 2020b). This is often achieved through a national risk assessment (NRA). NRAs provide security intelligence agencies with important typological information on corruption risk factors in the country, helping them to tailor their intelligence gathering and analysis at the strategic, operational, and tactical levels.

The results of the risk assessment also feature in the country's Mutual Evaluation Report (MER), which is either undertaken under the auspices of the FATF for its 37 FATF member countries[9], or one of the 9 FATF-styled regional bodies covering the rest of the world. This provides a detailed overview of ML risks, laws, policies and measures, and evidence of implementation of these systems, as well as an analysis of strengths and weaknesses of the country's AML/CFT/CFP framework. Corruption is a high priority area under the FATF Recommendations and is always directly covered in each MER. MERs are, however, not the end of the process. Follow-up Reports (FURs) are prepared at different frequencies, depending on how poorly the country did in its mutual evaluation. An FUR shows the progress of the country in addressing deficiencies outlined in the MER, as well as new issues prioritized globally by the FATF. FURs can, therefore, provide important context for intelligence agencies on underlying corruption issues currently faced by the country, and thus, should not be overlooked.

For countries with strategic AML deficiencies, the FATF publishes two lists known colloquially as "gray" and "black" lists[10]. The gray list identifies

[9] The FATF's 39 members also includes the European Commission and the Gulf Co-operation Council.

[10] The FATF "gray list" is titled "Jurisdictions under Increased Monitoring" while the "black list" is titled "High-Risk Jurisdictions subject to a Call for Action." Both lists are updated after the end of each FATF Plenary meeting which is held three times per year in February, June and October.

countries which have committed to address these deficiencies, and regularly report their progress in implementing an action plan agreed with the FATF. The most egregious cases find themselves on the black list, and are the subject of a call by the FATF for all 202 states in its network to apply countermeasures[11].

FURs may be required more frequently if, *inter alia*, there are deficiencies in one or more key FATF Recommendations related to corruption, including Recommendations 3 (Money Laundering Offence), 10 (Customer Due Diligence), 11 (Record Keeping by FIs), and 20 (Suspicious Transaction Reporting). These recommendations are also factors in deciding whether a country is placed on the gray list or the black list. MERs, FURs, and the FATFs' gray and black lists, therefore, form important OSINT for the intelligence community on corruption and related offences, providing a snapshot of corruption issues and measures to address or mitigate these risks. They can also point to other international partners who may have a deeper understanding of the situation on the ground.

Some jurisdictions or supra-national bodies also conduct their own evaluation of the AML/CFT/CFP risks posed by a country and the scope of which covers anti-corruption measures. The European Union (EU), for example, publishes its own list of high-risk third countries having strategic deficiencies in their AML/CFT regimes which could pose a threat to the EU internal market (European Commission [EC], 2020). In prioritizing countries for assessment, the EC considers reports from European Union Agency for Law Enforcement Cooperation (Europol) and the European Union External Action Service (EEAS), as well as other credible sources, regarding whether the country has significant levels of corruption (EC, 2016; EC, 2020). Europol has had a longstanding mandate on criminal intelligence coordination while the EEAS includes the EU Military Staff (EUMS). A subset of EUMS is the Intelligence Directorate which, *inter alia*, provides intelligence input into early warning and situation assessments (European Union External Action Service [EEAS], 2015). The EU's methodology also takes into account information provided by the

[11] For example, the FATF has called upon countries to apply counter-measures against the DPRK including enhanced scrutiny of business relationships and transactions with individuals and entities from the DPRK; applying targeted financial sanctions pursuant to relevant UN Security Council Resolutions; closing branches, subsidiaries and representative offices of DPRK banks within their territory; and terminating correspondent banking relationships pursuant to relevant UN Security Council Resolutions (FATF, 2020a).

intelligence services and FIUs of EU Member States in developing risk-profiles of third countries (EC, 2020).

Sanctions

On a final point related to AML measures, a foreign policy tool that is now being increasingly seen in the fight against corruption is targeted financial sanctions. Countries, such as the United States (e.g., the Russia and Moldova Jackson–Vanik Repeal and Sergei Magnitsky Rule of Law Accountability Act of 2012) and Canada (e.g., the Justice for Victims of Corrupt Foreign Officials Act) have enacted legislation that imposes autonomous sanctions on foreign corrupt actors, allowing for the freezing and returning of resources misappropriated by kleptocrats, and barring travel. Establishing sanctions is an intelligence-driven process, with policymakers relying on intelligence agencies and LEAs to provide the justification for applying these measures to targets. The intelligence community also has a role in assessing the effectiveness of sanctions on targeted countries, as well as to inform changes to sanctions policy (United States Government Accountability Office, 2019).

The Way Forward for the Intelligence Community

Corruption needs to remain a priority on the radar of the intelligence community. JCOA (2014) highlights lessons learned from the experience of the United States in dealing with issues related to corruption in Afghanistan. Some of the recommendations are useful, though not surprising, including legislative amendment to more clearly define US policy on corruption; clearly defining the military's role in combatting corruption; and improving corruption awareness and training within the military, including the impacts of corruption on post-conflict operations.

A key recommendation of the JCOA (2014) to improve intelligence across the operational continuum is taking a taskforce approach by forming multi-agency and multi-national intelligence cells focused on understanding the linkage between corruption, resource flows within the country, and criminal networks. A need to strengthen training for intelligence officers to integrate law enforcement skill sets to understand corruption within specific operational and cultural environments, was also identified. This is a useful recommendation granted the vast experience of law enforcement agencies, together with criminal intelligence units and FIUs, in gathering and analyzing corruption related intelligence, particularly financial intelligence at the strategic, operational, and tactical levels. It should also be noted that compliance professionals from FIs

and DNFBPs have a wealth of specialized experience, so this pool of talent should not be overlooked in seeking potential recruits for intelligence agencies.

The intelligence community also has an important role to play at the strategic level in preparing intelligence risk assessments on conditions abroad affecting their country's security and interests, outlining present and future threats. Intelligence risk assessments can encompass theaters where forces are or might be deployed, and terrorist operations affect national interests and other crises abroad. Corruption can impact all these issues as catalysts and enablers. Such strategic intelligence will guide not only military operations but also softer foreign policy tools to address corruption, ranging from diplomacy to targeted financial sanctions. The intelligence community also has an important role in assessing the effectiveness of such non-kinetic solutions which feeds into implementation and finessing of policy.

Finally, countries need to remain cognizant of the potential for corruption in their own civilian, military, law enforcement, and intelligence systems, as these present vulnerabilities which their enemies can exploit.

Author Note

The author has no known conflict of interest to disclose.
Correspondence concerning this article should be addressed to Andrew Dalip, Jr., email: maeson.chambers.law@gmail.com

Author Biography

Andrew Dalip, Jr. has practiced law in Trinidad and Tobago for over 22 years. He is a Certified Anti-Money Laundering Specialist and Certified Global Sanctions Specialist. He has undergone multiple trainings in anti-terrorism and is a trained assessor for the Financial Action Task Force (FATF) 4th Round Methodology. His experience spans development of domestic and international policy, all stages of legislative development, intelligence and investigative coordination, civil litigation, and criminal prosecution. As Special Legal Advisor to three Attorneys General, he held specific responsibility for anti-terrorism, WMDs, anti-money laundering, and applying targeted financial sanctions against terrorists and terrorist organizations. He led the development of policy and legislation to enact or amend several key laws, including the Anti-Terrorism Act and laws governing WMDs. He returned to private practice in 2018, and thereafter, serving as a strategic-level consultant, *inter alia*, anti-terrorism, anti-money laundering, combatting the proliferation of weapons of mass destruction, and sanctions.

References

Ahmad, E., Aman Ullah, M., & Irfanullah Arfeen, M. (2012). Does Corruption affect Economic Growth? *Latin American Journal of Economics*, 49(2), 277 – 305. http://dx.doi.org/1O.7764/LAJE.49.2.277

Best, R. (2010, December 7). *Securing America's Borders: The Role of the Intelligence Community*. Congressional Research Service. https://fas.org/sgp/crs/intel/R41520.pdf

Cabinet Office & Detica. (2011). *The Cost of Cybercrime*. Retrieved, October 4, 2020, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf

Chayes, S. (2014a). *Corruption: The Priority Intelligence Requirements*. Carnegie Endowment for Higher Peace. https://carnegieendowment.org/2014/09/09/corruption-priority-intelligence-requirements-pub-56572

Chayes, S. (2014b). *Corruption: The Unrecognized Threat to International Security*. Carnegie Endowment for Higher Peace, Working Group on Security and Corruption. https://carnegieendowment.org/2014/06/06/corruption-unrecognized-threat-to-international-security-pub-55791

Chivers, C. (2005, July 21). Soviet-Era Depots Tempting Terrorists. *The Moscow Times*. Retrieved, October 4, 2020, from http://oldtmt.vedomosti.ru/news/article/tmt/211135.html

Commission on the Theft of American Intellectual Property. (2017, February). *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy.* The National Bureau of Asian Research. http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

Defense Personnel Security Research Center. (2004). *Espionage Cases 1975 – 2004: Summaries and Sources.* Defense Counterintelligence and Security Agency. https://www.hsdl.org/?view&did=482512

Dobson, A. (2005, June). The Reagan Administration, Economic Warfare, and Starting to Close Down the Cold War. *Diplomatic History*, 29(3), 531-556.

European Commission. (2016, September 13). *First step towards a new EU list of third country jurisdictions: Scoreboard.*

https://ec.europa.eu/taxation_customs/sites/taxation/files/2016-0915_scoreboard-indicators.pdf

European Commission. (2020, May 7). *Commission Staff Working Document: Methodology for identifying high-risk third countries under Directive (EU) 2015/849*. https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/200507-anti-money-laundering-terrorism-financing-action-plan-methodology_en.pdf

European Union External Action Service. (2015, September). *EU Military Staff (EUMS): Contributing to European Union Foreign Policy*. http://www.eeas.europa.eu/archives/docs/csdp/structures-instruments-agencies/eu-military-staff/documents/web_version_eums_september_2015-jol_en.pdf

Financial Action Task Force. (2019, October). *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*. https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf

Financial Action Task Force. (2020, February 21). *High-Risk Jurisdictions subject to a Call for Action – 21 February 2020.* http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html

Financial Action Task Force. (2020, October). International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation: The FATF Recommendations. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Gates, M. (2020, July 1). An Unfair Advantage: Confronting Organized Intellectual Property Theft. *Security Management*, July 2020. https://www.asisonline.org/security-management-magazine/articles/2020/07/an-unfair-advantage-confronting-organized-intellectual-property-theft/

Joint and Coalition Operational Analysis. (2014, February 28). *Operationalizing Counter/Anti-Corruption Study.* https://www.hsdl.org/?view&did=756004

Lee, R. (2001, April 27). Nuclear Smuggling From The Former Soviet Union: Threats And Responses. *Foreign Policy Research Institute*.

https://www.bu.edu/globalbeat/nuclear/FPRI042701.html

McMahon, R. (2006, May 11). The Impact of the UN Oil-for-Food Scandal. *Council for Foreign Relations.* https://www.cfr.org/backgrounder/impact-un-oil-food-scandal

Military Watch Magazine. (2019, March 13). *Should Venezuela Transfer its F-16s to Russia? Exchanging U.S. Jets for MiGs Would Benefit both Caracas and its Moscow.* https://militarywatchmagazine.com/article/should-venezuela-transfer-its-f-16s-to-russia-exchanging-u-s-jets-for-migs-would-benefit-both-caracas-and-its-moscow

Nova Scotia Department of Justice Correctional Services. (2012, December 28). *Pre-Sentence Report: Queen vs. Jeffrey Paul Delisle.* https://assets.documentcloud.org/documents/602196/delisles-pre-sentence-report.pdf

Otterman, S. (2005, October 28). Iraq: Oil for Food Scandal. *Council for Foreign Relations.* https://www.cfr.org/backgrounder/iraq-oil-food-scandal

Sullivan, Mark. (2009, July 28). Venezuela: Political Conditions and U.S. Policy. *Congressional Research Service.* https://fas.org/sgp/crs/row/RL32488.pdf

Transparency International. (2014, February). *Corruption as a Threat to Stability and Peace.* https://ti-defence.org/wp-content/uploads/2016/03/2014-01_CorruptionThreatStabilityPeace.pdf

Transparency International. (2020, October 2). *For a more equal world post-COVID-19: Focus on the financial gatekeepers.* https://www.transparency.org/en/news/covid-19-inequality-illicit-financial-flows-gatekeepers-enablers

Transparency International Defence & Security. (2018). *Afghanistan: Corruption and the Making of Warlords.* https://iacg.ti-defence.org/casestudy/afghanistan-corruption-and-the-making-of-warlords/

Transparency International Defence & Security. (2019, November 18). *Corruption as Statecraft: Using Corrupt Practices as Foreign Policy Tools.* https://ti-defence.org/publications/corruption-as-statescraft/

United States Attorney's Office. (2018, December 11). *Press release: DEA Agent Arrested for Participating in Decade-Long Narcotics Conspiracy and Providing Firearms to Drug Trafficking Organization.*

https://www.justice.gov/usao-sdny/pr/dea-agent-arrested-participating-decade-long-narcotics-conspiracy-and-providing

United States Department of Justice. (2020, March 26). *Press release: Nicolás Maduro Moros and 14 Current and Former Venezuelan Officials Charged with Narco-Terrorism, Corruption, Drug Trafficking and Other Criminal Charges.* https://www.justice.gov/opa/pr/nicol-s-maduro-moros-and-14-current-and-former-venezuelan-officials-charged-narco-terrorism

United States Government Accountability Office. (2019, October 2). *Economic Sanctions: Agencies Assess Impacts on Targets, and Studies Suggest Several Factors Contribute to Sanctions' Effectiveness.* https://www.gao.gov/assets/710/701891.pdf

Von Clausewitz, C. (1832). *On War* (J. Graham, Trans.). New York, NY: Barnes & Noble.


This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

© Andrew, Dalip Jr., 2021

APA Citation:
Dalip, A. (2021). Intelligence and corruption. *The Journal of Intelligence, Conflict, and Warfare, 3*(3), 34-54.

Published by the Journal of Intelligence, Conflict and Warfare and Simon Fraser University
Available from: https://jicw.org/