



## **Survey of Experience with Transnational Organized Crime: Summary of Analyst and Educator Responses**

### **Introduction**

Transnational organized crime (TOC) refers to those self-perpetuating associations of individuals who operate across borders for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or through a transnational organizational structure and the exploitation of legal transnational commerce or communication mechanisms. There is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks to cells, and may evolve into other structures.

A high-level United Nations (UN) panel meeting in 2015 reinforced concerns about the impact of TOC upon peace processes. Though TOC is recognized as a global problem, it is addressed only to a small degree in a few UN mandates and sometimes finds its way into the planning process in New York. It is generally dealt with in a fragmentary manner and the response is incongruous with the importance of integrated planning and execution at the mission level.

Transnational organized crime mitigation is usually planned for in isolation from corruption and terrorism, but in complex missions the three are intertwined. Recent research strongly correlates the often symbiotic relationship among transnational crime, corruption, and terrorism commonly found in the environments where peacekeeping is required. Mission success is predicated upon a multidimensional/multidisciplinary approach toward UN missions and a clear division of labor between military and police in the planning stages, as well as finding or establishing complementarity among the various players, particularly when deployed to complex environments.

Within the UN, the Secretary General, Security Council, the Senior Police Advisor to the Department of Peacekeeping, and many others have noted the significant negative impact that transnational organized crime and terrorism have on the capability of the mission to comply with the Security Council mandate, especially as peacekeepers themselves have increasingly been attacked by both criminal and terrorist groups.

Similarly, the Global Initiative against Transnational Organized Crime, a network of law enforcement, governance and development practitioners serves as a platform to create a global strategy to counter organized crime, which published an input paper to the UN High Level Panel in February 2015 stating that the UN system appears to “lack the ability and determination to respond to organized crime.” The paper further noted that countering organized crime requires a focus on corruption as well and suggest the following to the UN:

- 1) Align political, economic, and judicial incentives and punishment measures to counter criminal engagement early in the peacebuilding process

- 2) Create prosecution capabilities at the national or regional level, similar to the piracy response
- 3) Reinforce regional or national prosecutions through mandating UN support for evidence-gathering
- 4) Build analytical capabilities that include conflict threat assessment and other tools that allow for proactive and preventative approaches to organized crime and its impact upon governance, development, and the state.

The recent presentation to the UN High Level Panel resulted in a call for a white paper, from The International Forum for the Challenges of Peace Operations to comprehensively address this complex triad and make recommendations to reduce the UN knowledge and capability gap, which appears to be at the mission level.

### **The Case for Analysis**

Through its extensive experience in fragile and post-conflict corrupt environments, PKSOI has generated the hypothesis that intelligence and criminal analysts are not always trained or equipped to recognize transnational organized crime (TOC) or the corrupt environment that nurtures it. PKSOI further posits that failing to do so diminishes effective forecasting and analysis, thus leading to mitigation strategies often developed at the policy level without full information from various sources, and without a complete picture of the environment through robust estimates derived through the use of proven analytic methods.

Through some cursory research, PKSOI had a difficult time identifying any specific organization within DoD focused on the global mission of identifying and mitigating TOC. There was also no apparent methodological approach to differentiating a TOC from a terrorist network, nor a common repository for integrating strategic intelligence with criminal intelligence to generate a more robust network analysis estimate.

To test this hypothesis, PKSOI developed a survey to gain a clearer understanding of analysts' experience at the operational and tactical levels. The survey also considered how training and education currently prepare analysts to effectively assess such complex environments using the most appropriate analytic tools. Although the survey response rate was too low to provide a significant sample, the responses received did anecdotally confirm PKSOI's assumptions:

1. Analysts identify, analyze and investigate many kinds of TOC networks, but lack formal training and do not apply proven analytic tools or techniques to the process
2. Educators report providing training at a more significant level than analysts report having received training
3. Training on specific types of crime mirrors the types of crime analysts are required to identify and have witnessed in the field, but there is likely a much higher magnitude of training needed than currently provided on many types of TOC

4. Analysts and educators tend to differentiate between TOCs and terrorist groups based on identified motive, i.e. greed vs. ideology; if they share characteristics, terrorist ties trump TOC interests for mitigation strategy development
5. There is little interest in identifying corrupt officials and others who may facilitate TOC, unless there is a terrorist connection

Analyst survey respondents received training on the following types of TOC: five on money laundering, four on cybercrime, three on drug smuggling, two on human trafficking and one on corruption. None were trained to assess antiquities, arms or wildlife trafficking, nor environmental crime or piracy.

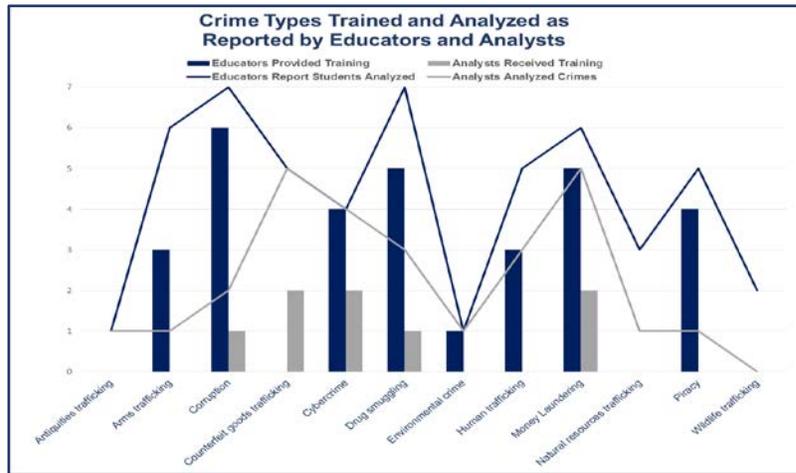


Figure 1. Analyst and educator responses on analysis and training conducted

Despite this lack of training, respondents identified, analyzed or investigated ALL of these crimes except wildlife smuggling. This results in a clear knowledge and skills deficit for those tasked to analyze and investigate all types of transnational crimes that undermine stability, as illustrated in Figure 1.

While it is highly likely that the analyst and educator groups do not overlap, they both report the same trend in types of crimes that have been analyzed, but the amounts of training claimed to have been provided by trainers and received by analysts is rather different. Only counterfeit goods trafficking and cybercrime are reported at the same volume by both groups. All respondents acknowledged having witnessed



Figure 2. Analyst responses on types of crimes witnessed and training received

most types of transnational crime included in the survey, whether or not they had worked in the field. However, the instances of first-hand observation far outweighed the instances of training on each type of crime, illustrating the magnitude of the dearth of criminality in comparison to analytic training, as noted in Figure 2. Two of eight educators self reported being “experts” in TOC and two of six analysts did the same.

## Tools and Products

In line with the lack of general training on TOC, analysts reported low use of specific tools commonly used to identify and analyze it; only one analyst claimed to use analytic tools such as Access, Excel and SSPS, and only one educator stated they use a combination of online proprietary data extraction tools.

As illustrated in Figure 3, both analysts and educators expressed familiarity with a variety of intelligence “products.” Two analysts used them in combination to respectively build cases and to alert investigators to financial crimes. However, many of these are collection reports, not finished intelligence products for decision makers, including those starred in Figure 3. The two reporting analysts stated that the consumers for their products are unspecified U.S. government agencies and anti-money laundering investigators respectively.

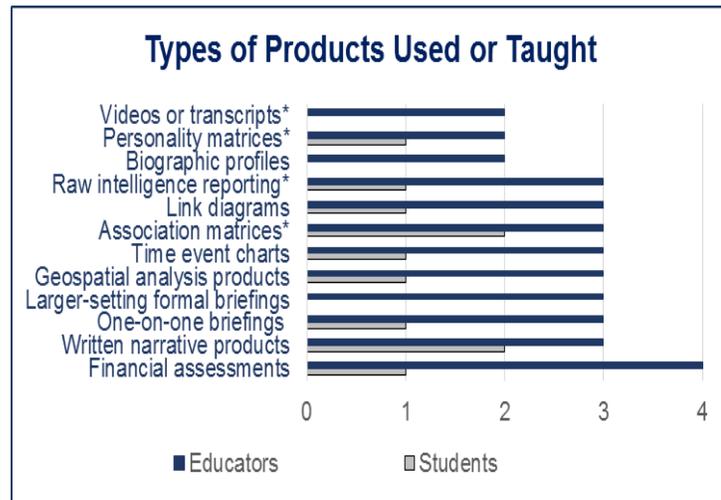


Figure 3. Reported use of intelligence “products”

## Differentiating between TOC and Terrorist Groups

Four of the five educators who responded to the question of how they differentiate between TOC and terrorist groups pointed to motive of the organization as the primary identifier. One respondent noted that either type could possess *both* ideological *and* profit motivations; another respondent suggested that the level of international state actors supporting their activities was the determining factor.

In terms of classifying facilitators who span or conjoin both types of networks, the educators agreed that they share characteristics of both groups, but that there is little value in studying them past motive identification as involvement in terrorist activities becomes the only implicating factor of interest. There were no clear responses to the questions on integrating criminal and tactical or strategic intelligence products for more robust network analysis or on identifying corrupt officials facilitating TOC.

***The flow of organized crime (guns, drugs, people, ivory, etc.) is transnational; however, the control of the flow is local.*** Thus, a paper that addresses the mission’s ability to identify, analyze and investigate organized crime, corruption, and terrorism and use tested methodologies to determine the appropriate mission responses will fill a very real gap in knowledge and capabilities to improve peacekeeping effectiveness and potentially reduce its need in future missions.