HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

POLICY PAPER
belfercenter.org/homelandsecurity

HOMELAND SECURITY PROJECT | MARCH 2021

Disrupting Transnational Criminal Activity

A Law Enforcement Strategy for Homeland Security

Alan Bersin and Chappell Lawson

Executive Summary

Transnational criminal activity, organized or not, presents a substantial internal security threat to the United States as it does to other nation-states across the world. Combating it remains a critical mission in the homeland security enterprise. Federal efforts across that enterprise, however, remain scattered and largely ineffectual, and many types of transnational crime are resistant to the law enforcement tactics used domestically.

This paper proposes that the U.S. Department of Homeland Security (DHS) take the lead in supplementing the traditional "criminal justice" approach to countering transnational crime with strategies that aim to disrupt it and insulate Americans from its harmful effects. We contend the "Disruption Model" outlined here,* if broadly implemented, could significantly complement the current conventional approach, and produce materially improved results in managing the challenges of transnational crime and protecting the homeland from its ravages.

* The ideas in this policy brief are developed in greater detail in Alan Bersin and Chappell Lawson, "Homeland Security and Transnational Crime," in Chappell Lawson, Alan Bersin and Juliette Kayyem, eds., *Beyond 9/11: Homeland Security for the Twenty-First Century* (Cambridge, MA: MIT Press, 2020).

Background

Transnational Crime and the Underworld of Globalization. Unlawful flows on a massive scale, engineered by transnational criminal organizations (TCOs), generate enormous revenues that support and perpetuate a vast and growing infrastructure of "dark commerce" that has developed in parallel with the process of globalization. This has resulted in a global netherworld of borderless criminality that increasingly is digitally facilitated.[1]

The U.S. National Security Council estimates $1.3 trillion to $3.3 trillion is involved in money laundering perpetrated by transnational criminal enterprises; $750 billion to $1 trillion in narcotics trafficking; $170 billion to $320 billion in illicit firearms trafficking; $21 billion in human trafficking; $500 billion in counterfeit and pirated goods; $20 to $40 billion in environmental crimes including illegal wildlife trade; and $10 to $12 billion in fraudulent credit card transactions. The total proceeds of transnational organized crime are estimated at $6.2 trillion or about 10 percent of gross global product. This amount approaches the total 2017 gross domestic product of all the countries in Africa ($2.9 trillion) and South America ($3.99 trillion) combined. Bribery of corrupt officials internationally is estimated to amount to $1 trillion annually.[2]

TCOs and their illicit economies thrive in the spaces between nation states and the interstices of lawful trade and travel. They exploit the inability of any one nation state acting on its own to control their far-flung operations. The reticence of nation states to provide adequate authority and resources to multilateral law enforcement organizations, such as INTERPOL, limits as well any reasonably satisfactory collective containment of transnational crime globally. TCOs' use of modern means and methods—including cyberspace, cryptocurrencies, and encrypted communications—further conceals and protects syndicate activities and operatives.[3]

The gaps in global governance to counter transnational criminal activity are paralleled by deficits within the domestic regulatory and law enforcement regime in the United States. Non-state actors operate not only in the spaces between nations but also in the seams between their domestic national security and defense and law enforcement establishments, and their respective "stove-piped" authorities and operations. This incapacity at national and international levels alike to control TCOs gives rise to the proposal advanced here on a revised approach to more effectively managing transnational crime and containing its consequences to the homeland.[4]

Analysis

The U.S. Framework Countering TCOs and Transnational Crime. Federal efforts geared to combating transnational crime remain divided among various agencies in three different Cabinet-level departments, specifically:

- the Drug Enforcement Administration, or DEA (Department of Justice (DOJ))
- the Federal Bureau of Investigation, or FBI (DOJ)
- the Bureau of Alcohol, Tobacco, Firearms and Explosives, or ATF (DOJ)
- Homeland Security Investigations (HSI) at Immigration and Customs Enforcement, or ICE/HSI (DHS)
- Customs and Border Protection, or CBP (DHS)
- the Secret Service, or USSS (DHS)
- the U.S. Coast Guard, or USCG (DHS)
- the Financial Crimes Enforcement Network, or FINCEN (Department of Treasury)
- Internal Revenue Service, Criminal Investigative Division, or IRS-CID (Department of Treasury)

As their names imply, these agencies each have their own specific focus; for instance, the DEA's investigative efforts concentrate on crimes related to narcotics. However, there often is overlap in the types of cases these agencies can pursue. ICE theoretically can investigate, for example, any case with a "border nexus," including within its jurisdiction a wide range of criminality from drugs and human trafficking to child pornography and stolen antiquities. Concerns that other investigations will interfere inadvertently with a criminal, counterintelligence, or counterterrorism case being developed against a set of perpetrators ordinarily limits routine information-sharing among these agencies.

Post-9/11 reforms that fundamentally altered the government's approach to terrorist networks—and dramatically enhanced information sharing, for example, between the Central Intelligence Agency (CIA) and the FBI on terrorism—had virtually no effect on federal operations against purely criminal activities. This latter enforcement arena remains wedded to the generation of "cases" centered on extended investigations, prosecutorial charging discretion, and the presentation of evidence at trial. Agencies, accordingly, endeavor to stay out of each other's lanes and, only occasionally, operate cooperatively on a single investigation through a "coalition of the willing" centered in a task force.

U.S. agencies engaged in countering transnational crime follow one of two strategies and, usually, some combination of the two: (a) utilizing the traditional criminal justice model which relies on the conventional "investigate-indict-arrest-prosecute-punish" approach and/or (b) interdicting contraband on identified smuggling routes for purposes of seizure or further use as "controlled deliveries" within a larger investigation. These approaches are designed for take-downs against hierarchically structured groups (transnational ***organized*** crime). The second approach, in particular, aims at smuggling operations and preventing the cross-border entry of contraband, principally narcotics, into the country. These standard operating procedures rarely reflect broad strategic planning or deep operational coordination across agencies.

Such approaches are ineffective, for the most part, against most transnational crime, for one or more of several reasons:

1. **Extraterritoriality**: Those who orchestrate criminal activities frequently reside in safe harbors outside the United States where extradition is not available. This challenge is particularly evident in the rapid expansion of web-enabled criminality. Cyberspace permits networked malefactors both to ignore national boundaries in the plying of their criminal craft and to avoid crossing physical borders where their apprehension is possible. As a result, domestic law enforcement operations increasingly have limited impact on the cost/benefit calculus conducted by criminal elements abroad. The remote prospect for arrest and punishment—"cuffing the criminal"—at the hands of U.S. authorities, therefore, remains inadequate to deter many forms of harmful transnational activity.[5]
2. **Criminal Syndicate Business Continuity**: Transnational criminal activity is either highly dispersed and carried out by loose networks (particularly cyber-crime) or controlled by hierarchically structured organizations. Darknet marketplaces and cryptocurrencies are decentralized, and criminal cyberspace operations increasingly are decentralized to avoid a centralized takedown from law enforcement. Even where crime is organized tightly and its leadership centralized, the impact of a "decapitation" strategy is short-lived. Following the arrest of a mob boss, power passes quickly to a successor, designated or not, inasmuch as the illicit revenue stream remains intact. These proceeds provide a powerful incentive to maintain the organization and continue its criminal activities. The case of Chapo Guzman and the Sinaloa Cartel illustrate the typical absence of sustained results from the "take down" of a "kingpin" on the continued operation of illicit activity.
3. **Scale of Illegal Activity**: Many manifestations of transnational crime are conducted at a volume and level of activity that defy conventional enforcement responses under the criminal justice model. Undocumented migration, narcotics consumption and sales, child pornography, and other cyber-enabled crimes, for example, are not problems that the federal

government, or society, can arrest their way out of or control satisfactorily through prosecution and imprisonment. The choice of a specific target for the exercise of police or prosecutorial discretion often is not informed by a broader strategy or set of policy considerations. This opens the door to widespread perception among growing segments of the public that the generation of leads is either happenstance and/or the result of discriminatory target selection.

The current approach to transnational crime appears, therefore, both outmoded and ineffective, and in need of an alteration in paradigm. DHS should shift its approach in our view to focus on how best to disrupt transnational criminal activity, and dismantle transnational organizations, using all the tools at its disposal that are available through broad search and seizure authorities at the border. Given these authorities, and the border security mission central to homeland protection, DHS and its component agencies (CBP, ICE, USCG and TSA) are better placed than counterparts at Justice or Treasury to shift away from complete reliance on the criminal justice model.

Although "take down" operations and seizures would remain important elements in countering transnational crime, they would not be the only strategies applied. Greater attention would be placed on tactical means and methods geared to disrupting TOC operations, such as preventing travel by criminals, interfering with cartel communications, seizing illicit product and destroying its source and, perhaps most importantly, disrupting financial dealings and breaking up money laundering networks and arrangements.[6] Table 1 summarizes the differences between the existing approach and the one advocated here.

Table 1: A Comparison of Current Approaches to the Disruption Model

	Conventional Approach	Disruption Approach
Goals and Doctrine	Put the worst actors in jail and seize contraband shipments; focus on powerful organized crime groups.	Impede and disrupt transnational crime, whether organized or dispersed; and dismantle criminal organizations and infrastructure.
Metrics of Success	Arrests, indictments, prosecutions, convictions, and volumes of contraband seized.	Diminution of criminal activity; increased difficulty for criminal networks to operate; and measurable reduced adverse impact on homeland communities.
Data	Gather information that can be converted into admissible evidence to make cases in court.	Use Big Data, incorporating all federal government data streams, and advanced analytics to characterize criminal networks, generate investigative leads and customize optimal operational responses.
Information-sharing	Limit sharing to protect cases and sources; focus information-sharing principally on de-confliction.	Combine information from as many sources as possible to identify criminal activity, map criminal networks, and develop calculated responses.
Legal Authorities	Narrow search authorities based on U.S. law and inability, absent judicial approval, to materially restrict the movement of suspects.	Broad border-related search authorities with wide discretion and capacity to impede international travel by suspects and detain goods and cargo at ports of entry.
Operational Protocols	Limited coordination in take-down operations, but cases typically "belong" to one agency, with only ad hoc investigative collaboration.	Efforts at disruption are coordinated across the whole of government in a strategic, systematic fashion.
Training and Professional Development	Training focuses on standard investigative techniques.	Analysis of criminal business models, law enforcement intelligence, and investigative and operational counter-TCO strategy and planning.
Career Pathing	Promotion is based on participation in large investigations involving arrests, seizures, prosecutions, convictions, and imprisonment of TCO members through use of conspiracy doctrines.	Promotion, reward, and recognition are based on identifying vulnerabilities in criminal networks, devising the best operational response aimed at weakening the TCO support infrastructure, and decreasing the harmful impact of transnational criminal activity on the homeland.

Integrated Whole of Government Counter-Transnational Crime Effort. There are five dimensions of official power available to enlist in support of a disruption strategy: (a) intelligence collection and analysis; (b) law enforcement response; (c) financial sanction; (d) diplomatic partnership with foreign governments; and (e) direct action. For a Disruption Model to work, an explicit Presidential Policy Directive (PPD) would be required to create an interagency policy mechanism to knit these forms of power into a coherent strategy. This framework in turn would ensure that information is more broadly shared across federal agencies and analyzed in a more sophisticated way. Disruption also requires changes in doctrine, metrics of success, training, and career pathing, as well as changes at CBP's National Targeting Center (NTC) and in other intelligence and risk management functions.[7]

The U.S. Government's whole of government response to the threat of terrorism developed during the past twenty years provides ample precedent for the kind of changes advocated here. Campaigns, spearheaded by the military and intelligence communities but coordinated across the government, have significantly weakened jihadists—whether al Qaeda or D'aesh—and their capabilities for attack. Similar efforts directed against terrorist finances led by civilian agencies have resulted in widespread success in well-coordinated operations involving the public and private sectors.

Moreover, the counter-terror finance campaign has deployed directly the disruption model in order to achieve their objectives when application of the traditional criminal justice model is not feasible. In a landmark effort announced publicly in August 2020, three terror finance cyber-enabled campaigns were disrupted, resulting in the largest ever seizure of cryptocurrency accounts held by terrorist organizations. According to the Department of Justice, "terror finance campaigns [conducted by the al-Qassim Brigades, Hamas's military wing, al-Qaeda, and Islamic State of Iraq and the Levant (ISIS)] all relied on sophisticated cyber-tools, including the solicitation of cryptocurrency donations from around the world."[8]

To defeat this terrorist cyber crowdsourcing, agents from DHS, Treasury, and DOJ working in close concert with a federal prosecutor, devised and executed a novel set of disruptive actions, customizing existing legal tools and authorities to place them into action. The strategy included: (a) using the All-Writs Act to launch a denial-of-service (DOS) attack against a targeted website; (b) operating an undercover Terrorist Donation website to divert contributions; (c) seizing and taking over various online accounts (e-mails, web servers, etc.) to confuse and disrupt communications; and (d) making undercover Bitcoin donations in order to facilitate tracing of the money (laundering) flows key to the terrorist scheme.[9]

We submit that these and analogous tools, techniques, means, and methods—appropriately tailored and customized—are relevant to the challenge of transnational criminal activity across the board

and should be systematically adapted to policing and investigative strategies aimed at countering it. A series of recommendations to this end follow.

Recommendations

Recommendation 1: The President should issue a Presidential Policy Directive (PPD) supporting the implementation of a disruption strategy to counter transnational organized crime on a "whole of government" basis.

Left to their own devices, the departments and agencies responsible for countering transnational criminal activity will not implement on an acceptable timeline, if at all, a paradigm change in their enforcement model. The current culture and institutional incentives are too strongly rooted in the traditional criminal justice approach, and the bureaucratic resistance to change is substantial. It will thus take leadership at the highest level of government to mandate a change, identify the necessary steps, and monitor and enforce compliance with the revised strategy. The PPD must identify clear actions required of each department and agency along with metrics that will allow the National Security Advisor to monitor implementation of the strategy.

Of particular importance is providing direction on the application of lessons-learned from counter-terror finance to disrupt criminal finance as effectively. Concerns about adversely impacting banks and other financial institutions have often prevented effective action in the past—but it is time to highlight directly the crucial importance of effective anti-money laundering enforcement. Significantly disrupting criminal finances is a core component of the disruption strategy, and it is a necessary condition to materially reducing the power and activities of TCOs.

Recommendation 2: The White House must establish a robust staffing structure to oversee implementation of the PPD through the National Security Council staff.

The NSC staff has directorates dedicated to border security and transnational criminal issues, but they currently have neither the institutional clout nor the expertise to manage the creation and implementation of a disruption strategy. We are agnostic to how precisely to structure a strengthened transnational crime capacity at the NSC, other than that it must be led by a very senior and

experienced official with direct access to the National Security Advisor and Homeland Security Advisor, along with backing of the President to direct change at the involved departments and agencies.

The new staff must oversee an interagency group charged with breaking down barriers to information-sharing across federal law enforcement agencies. This group should spell out the nominations process for the transnational crime watchlist and outline response protocols for when watch listed individuals are encountered. It should also identify how the Consolidated Priority Organization Targets (CPOT) process for directing conventional investigative efforts against organized crime groups can be used to identify candidates for the watchlist.

With the addition of representatives from the Intelligence Community, this group should (a) identify intelligence requirements for combating transnational crime and (b) consider how tools designed to map terrorist networks and trace terrorist financing may be transferred to the transnational crime context. It should also coordinate and oversee whole-of-government efforts against specific types of transnational crime (e.g. human trafficking), and engage state, local, and foreign partners in such efforts.

Recommendation 3: DHS needs to develop a policy and personnel infrastructure to execute its responsibility as the lead department in the disruption strategy.

The disruption strategy, as explained above, does not require abandoning the traditional criminal justice model. Instead, it pairs with that traditional approach a new set of tools and focus to attack criminal groups where they are most vulnerable: at the border. As the cabinet department responsible for border security, DHS necessarily will play a lead role in creating the policy framework required to implement a disruption model.

The plan will also need to create an institutional capacity within DHS for operational coordination against criminal networks. This coordination would encompass both interdiction (CBP and Coast Guard) and investigative functions (ICE and Secret Service), with liaison mechanisms for reaching out to and involving other federal, state, and local law enforcement resources and capabilities.

As DHS approaches this new role, it must learn from and nurture the programs and entities currently involved in disruption-like operations, of which there are notable examples. These include the CBP' National Targeting Center (NTC) (which identifies high risk passengers and cargo); ICE/HSI "cyber" takedown programs; the Border Enforcement Analytics Program (which uses cargo

data to identify potential criminal networks); the Human Smuggling Cell (which aims to discourage decentralized human smuggling); and the Bulk Cash Smuggling Center in Vermont. As the disruption strategy matures, DHS must ensure that these types of programs are operating harmoniously together and connected.

DHS, along with other federal law enforcement, must also address the programs that are not working rather than permit ineffective programs to continue. Either agencies reform the programs to make them effective, or they should be disbanded or moved to agencies that will use them to achieve measurable results in accordance with the disruption strategy.

Recommendation 4: The federal government must strengthen its abilities to identify criminals in the flows of international travelers and disrupt their travel.

Preventing criminals, along with their associates and beneficiaries, from engaging in cross-border travel is a powerful tool to curb TCOs. Although much criminal activity can be accomplished remotely, travel is often necessary operationally and restricting criminal movement will create opportunities to target and arrest criminals as well as to disrupt their activity. Accordingly, the PPD should instruct the DHS Office of Policy, DHS Office of Intelligence and Analysis, and the National Vetting Center (NVC), with the participation and support of the full federal law enforcement community, to develop a watch-list for transnational criminals, akin to that for terrorists.

CBP, through its National Targeting Center, must also place a greater emphasis on identifying transnational criminal activity (though without drastically reducing its counterterrorism efforts). To overcome the resistance other agencies have to working with CBP (which arises from a fear that CBP will compromise an investigation or case), CBP should involve its interagency partners in the governance of the NTC as has been done in the NVC.

Recommendation 5: The United States needs to lead the world in confronting transnational crime and take concrete steps to engage its allies in a strategy of disruption.

The United States cannot solve the TCO problem alone. By definition, the problem is transnational and frequently resides outside the jurisdiction of the United States. An effective international engagement strategy is, therefore, crucial.

As initial steps, the new NSC staff should, with the endorsement of the White House, take the lead in (a) developing bilateral information-sharing agreements with foreign governments to monitor the travel of suspects and make nominations for the transnational crime watchlist and (b) working with the World Customs Organization, INTERPOL, and other bodies to establish more robust mechanisms for multinational cooperation against transnational crime.

While the U.S. government pursues these institutional relationships and changes, DHS, along with the Departments of State and Treasury, and the Intelligence Community, should be working to establish operational connectivity with partner countries. The Department of Justice, in particular the FBI and DEA, have some of the most robust international law enforcement relationships, and they must be engaged. DHS's Office of International Affairs will need to work with DHS Components to develop training for DHS attachés abroad, so that they properly understand and prioritize disruption over the conventional model.

About the Authors

Alan Bersin has held numerous high-level positions at the U.S. Department of Homeland Security and U.S. Department of Justice. Most recently, after serving as the Commissioner of U.S. Customs and Border Protection, Bersin served as the Assistant Secretary for Policy and Chief Diplomatic Officer for DHS. Previously, he was the U.S. Attorney for the Southern District of California. He also served as a Vice President for the Americas and on the Executive Committee of INTERPOL. Bersin is a Global Fellow with the Wilson Center and a Senior Fellow with the Belfer Center at the Harvard Kennedy School.

Chappell Lawson is an Associate Professor of Political Science at the Massachusetts Institute of Technology, where he directs the MIT International Science and Technology Initiatives (MISTI) program and the International Policy Lab. Dr. Lawson has served in senior positions in government, most recently as the Executive Director of Policy and Senior Advisor to the Commissioner of U.S. Customs and Border Protection. He also served as a Director of Inter-American Affairs on the National Security Council staff during the Clinton Administration.

Acknowledgements

The authors acknowledge gratefully the thoughtful review of the original article, as well as this policy brief, by Ryan Landers, Supervisory Special Agent, Homeland Security Investigations, U.S. Department of Homeland Security.

Notes

1 Louise Shelley, *Dark Commerce: How A New Illicit Economy is Threatening Our Future* (Princeton, NJ: Princeton University Press, 2018).

2 *See* U.S. National Security Council, *Strategy to Combat Transnational Organized Crime* (Washington, DC: The White House, 2011). Transnational criminal activities remain so opaque and non-transparent that estimates of their proceeds remain no more than educated guesses subject to wide disparity. In contrast to the NSC, the United Nations Office on Drugs and Crime estimates TCO proceeds far less at $870 Billion, or 1.5 percent of gross global product. *See* United Nations Office on Drugs and Crime, *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes* (Vienna, October 2011), available at https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

3 United Nations Office on Drugs and Crime, *Globalization of Crime: A Transnational Organized Crime Threat Assessment* (Vienna, 2010); Louise Shelly, "Transnational Organized Crime: An Imminent Threat to the Nation-State?" Journal of International Affairs 48, no. 2 (winter 1995). *See also* U.S. National Security Council, *Strategy to Combat Transnational Organized Crime*; Andreas M. Antonopoulos, *The Internet of Money* (Merkle Bloom, LLC, 2016).

4 Alan Bersin and Lars Karlsson, "Lines, Flows, and Transnational Crime: Toward a Revised Approach to Countering the Underworld of Globalization," *Homeland Security Affairs* 15, art. 6 (December 2019), *available at* www.hsaj.org/articles/15514.

5 Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, (New York, NY: Simon and Schuster, 2016).

6 Martin Innes and James W.E. Sheptycki, "From Detection to Disruption: Intelligence and the Changing Logic of Police Crime Control in the United Kingdom," *International Criminal Justice Review*, vol. 14 (May 2004): 13.

7 Alice Hutchings and Thomas J. Holt, "The Online Stolen Data Market: Disruption and Intervention Approaches," *Global Crime*, vol. 18, no. 1 (2017): 12.

8 U.S. Department of Justice, Office of Public Affairs, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," press release, August 13, 2020.

9 Ibid.