The State as a Transnational Criminal Organization

A North Korea Case Study

Maj Brian Hill, USAF

Abstract

Throughout history, many states have tolerated, sponsored, or even partnered with transnational criminal organizations, but the Democratic People's Republic of Korea (DPRK) stands out as a nation where the government itself *is* the criminal organization, directly conducting drug trafficking, counterfeiting, money laundering, and other criminal enterprises. These activities have direct destabilizing effects and contribute to the DPRK's ability to circumvent sanctions and fund its illicit nuclear weapons program. Moreover, this condition of the state as the criminal organization poses a unique challenge to the international community, requiring a different approach for analyzing and combating the problem. This article explores this phenomenon with a brief historical review of state involvement in transnational crime, then brings together multiple previous analyses to provide a more comprehensive examination of the DPRK as a distinctive case study. It concludes by offering recommendations for further examination and action to counter this destabilizing force that undermines economies and strains national and international security structures.

***

What happens when a state not only allows, sponsors, or partners with transnational criminal organizations (TCO) but *is* the transnational criminal organization? How does one deal with an international crime boss who also serves as the head of state for the world's most isolated nation?

Transnational organized crime (TOC) is a destabilizing force that undermines economies and strains national and international security structures. Hostile states are increasingly turning to TOC as an asymmetric tool of power, presenting a key threat to US national security. This trend of state-operated TOC (SOTOC) will continue to increase in conjunction with global connectivity and as less powerful or economically viable states continue seeing benefit in using criminal activity as a balance against more powerful states. Though it is a form of TOC, SOTOC presents unique challenges that can neither be analyzed nor addressed the same way as traditional TOC. One of the most salient modern examples of this phe-

nomenon is North Korea, a nation whose state apparatus is directly involved in trafficking, counterfeiting, and cybercrimes.

This article examines why policy makers and researchers must view SOTOC, its analysis, and its potential solutions differently than either traditional TOC or a hostile government. First this article defines several key terms and scopes the discussion of SOTOC. Then it briefly discusses the historical and modern context of SOTOC. This section will focus on North Korea as a prominent example of modern SOTOC, a state that actively operates trafficking, counterfeiting, and cybercrime enterprises. Finally, the piece concludes with a discussion of why the United States and its allies must analyze and address this problem differently than the TOC conducted by independent TCOs and provide suggestions for doing so both for the DPRK and beyond.

Defining State-Operated Transnational Organized Crime

There are several academic definitions of *transnational organized crime*, but for the purposes of this discussion we will utilize one similar to the *US Strategy to Combat Transnational Organized Crime* definition, with some simplifications. TOC will be considered criminal activity, conducted by an organization, that crosses national boundaries and is motivated by some form of material profit. A *transnational criminal organization* will be defined as a nonstate organization that conducts TOC. SOTOC refers to TOC that is directly operated and sanctioned by a state as part of its official policy. Thus, this article does not focus on states that are simply permissive or complicit in the commission of organized crime by nonstate actors but rather ones in which the state is the primary driver of the criminal activity itself. Further, the article does not address the concept of a state as an exploitative entity toward its own population as described by sociologist Charles Tilly,[1] nor will it address genocide and other crimes against humanity as described in the 1945 Charter of London, which guided the Nuremberg Trials and the United Nation's guiding documents for the International Criminal Tribunal for Yugoslavia and, later, Rwanda, and which discuss the state as an organized criminal actor in the context of genocide.[2] This human-rights–focused definition of the state as an organized crime actor has become more common in recent decades and features a growing field of scholarship.[3] These additional definitions are valid, but this article foregoes these discussions and focuses on organized crime in a more traditional context involving profit-motivated entities.

To properly scope this discussion, there are essentially four levels of state involvement in criminal activities. The first is *passive complicity*, wherein a state turns a blind eye toward the activity due to corruption, fear, or simply an inability to act. The second is *encouragement*, where the state sees some form of value to itself in

the activity but is not willing to provide overt support. The third is *state-supported* or *state-sponsored*, in which the state provides financial, material, or other forms of support to the criminal activity. Finally, there is *state-operated*, which is criminal activity directed by the state and conducted through groups that report to the state, either directly or through indirect methods meant to obfuscate state involvement. This fourth category sits at the extreme end of the concept of the *criminalized state* put forward by journalist and national security consultant Douglas Farah and is how this article will define SOTOC.[4] However, it should also be noted that the line between the third and fourth levels is often blurry, particularly since governments typically try to obfuscate their involvement in criminal activity.[5]

States' Involvement in Transnational Organized Crime

SOTOC is not a new phenomenon. Letters of marque for privateers date back centuries and constitute a concerted effort by states to leverage criminal elements against their enemies.[6] The state was not merely endorsing these criminal activities. Rather, the state was actively directing them, falling squarely into the SOTOC category. Similarly, France actively engaged in opium smuggling to support its colonization of Indochina.[7] Smuggling of illicit goods, particularly arms, remains the most widely reported form of SOTOC. The Iran-Contra Affair is a particularly notable example, wherein the US executive branch violated domestic and international laws to provide weapons to Iran and funding and weapons to the Contra insurgency in Nicaragua.[8] Today, state-operated cybercrime is becoming increasingly ubiquitous and includes influence operations, espionage, sabotage, and profit-motivated cybercrime such as extortion via ransomware.[9]

All these forms of SOTOC have similar motivations as any other asymmetric means of conflict. States that are willing to leverage all instruments of power through creative means can overcome a conventionally more powerful opponent.[10] States that are militarily weaker in a conventional sense sometimes turn to state-sponsored or state-operated terrorism to provide an offsetting capability. Similarly, states can leverage TOC to offset disadvantages in the security and economic realms.[11] Also like terrorism, this can be done via proxy or with varying levels of state support and state direction, and this phenomenon is observed in several South American countries, most notably Venezuela and Suriname.[12]

The DPRK: A Unique Criminal Enterprise

However, the single most extreme example of a state actively operating as a TCO is the Democratic People's Republic of Korea (DPRK). In fact, the DPRK

may be more actively engaged in criminal activity than any other nation, and Paul Rexton Kan, Bruce E. Bechtol, Jr. and Robert M. Collins characterize North Korea as particularly unique among states that leverage TOC.[13] By comparison, while the Chinese government may turn a blind eye toward some counterfeiting activity that occurs within its borders and narcotics traffickers partner with some South American governments, the DPRK's government takes an even more active role in these activities, directs their execution, and can even be credited with the initial establishment of its criminal enterprises. This state-controlled crime purportedly occurs across a wide portfolio that includes drug manufacturing and trafficking; weapons trafficking; counterfeiting of goods, pharmaceuticals, and money; endangered species trafficking; insurance fraud; and human trafficking, though some are more clearly linked to the regime than others.[14]

Reports of the DPRK's drug production and trafficking are fairly extensive prior to 2003, with large shipments of methamphetamine and heroin seized and linked directly to the DPRK over the preceding three decades. Since 2003, however, there have been no direct links established between the DPRK and drug shipments. This may be a direct result of the seizure of drugs on the DPRK-flagged vessel *Pong Su* that occurred that year, after which the DPRK government may have reduced its drug activity to avoid further sanctions and scrutiny. However, it may also be a result of partnerships with Chinese criminal organizations that may now be facilitating the movement of drugs, adding an additional layer of obfuscation and making it more difficult to link the drugs to the DPRK.[15] Additionally, the overall shift toward horizontal integration among narcotics traffickers seen around the world may have influenced a change in how the DPRK conducts its own trafficking operations, shifting it from a purely state-owned enterprise to a state-sanctioned one.[16]

There is similar ambiguity in counterfeit pharmaceuticals, a field where both China and the DPRK have been implicated as sources for the products with the actual point of origin remaining unclear.[17] However, if the counterfeit pharmaceuticals were sourced from the DPRK, the advanced pharmaceuticals industry in the DPRK and its direct ties to the government imply significant involvement by the government in their production. In addition to counterfeit pharmaceuticals, the DPRK is likely also involved in the production and distribution of counterfeit cigarettes, with some sources indicating the DPRK is one of the largest producers of counterfeit cigarettes in the world.[18] Probably the most prominent field of counterfeiting in which the DPRK has been implicated is US currency. The United States previously accused it of manufacturing US $100 "supernotes," though other sources state the evidence for this is tenuous.[19] Nevertheless, there have been numerous counterfeiting incidents tied to the DPRK and indications

that even as far back as the 1950s the DPRK was counterfeiting South Korean currency.[20] Additional reports suggest links between the DPRK regime and both human and endangered species trafficking, though the degree to which the regime itself is involved in these is unclear.[21]

Finally, the DPRK is heavily involved in cybercrime. This is not unusual for many states, with nations committing cyberattacks on infrastructure and conducting intrusion into government and commercial networks for the purpose of military, industrial, political, and economic espionage. The DPRK has been implicated in such operations as well but also leverages crime in cyberspace for the more classic criminal purpose of profit. A cyber robbery in which USD 100 million out of an attempted USD 1 billion was stolen from the Bangladesh Bank via the Federal Reserve Bank of New York was linked to the DPRK.[22] UN reporting indicates North Korean hackers directly stole USD 50 million in cryptocurrency in 2020, which was likely funneled into its nuclear weapons program. Other reports from April 2022 link the DPRK to a USD 615 million cryptocurrency theft. All reports consolidated suggest the DPRK has stolen billions in cryptocurrency.[23]

The DPRK's driving motivation is clear: economically, the regime is extremely weak from a conventional sense. A combination of international sanctions and its own reclusiveness and insistence on self-reliance combine to keep the DPRK's economy closed off from much of the world. Pyongyang has taken some steps to change this and engages in limited trade, with China as its primary partner, but runs at a steep deficit and does not generate enough income to support a robust economy. North Korea's internal economy also remains weak and continues to decline according to estimates by the Bank of Korea in South Korea.[24] States that are militarily weak on the conventional side often turn to asymmetric activities like state-sponsored terrorism. Similarly, the DPRK has turned to transnational criminal activity to bolster its funding, with the primary concern from analysts being that these additional funds are funneled into its nuclear weapons program.[25] Thus, this goes beyond the typical construct of corrupt government officials profiting from criminal activity. Rather, the state apparatus itself is the TCO.

Combating SOTOC: Beyond Traditional Countermeasures

This poses unique challenges when determining how to combat this form of organized crime. Distinguished fellow at the Carnegie Endowment for International Peace Moisés Naím proposes several key activities for combating TOC, including reducing corruption, leveraging nongovernmental organizations (NGO), enhancing tracking technology, and partnering with other nations to present global solutions.[26] Some tactics, like improving cybersecurity and cutting off the supply of counterfeit currency while improving detection and removal of

that which is already in circulation are fairly straightforward at addressing cybercrime and monetary counterfeiting, respectively. Unfortunately, many of the other counter-TOC strategies become much more difficult or entirely ineffective when confronted with SOTOC.

Attempting to reduce corruption in the host nation is a key tactic in combating TCOs but is entirely moot in the context of the state acting as the TCO. Corrupt officials are not the problem, since the state apparatus as a whole is conducting these operations. Therefore, such a tactic would be like trying to combat a drug trafficking cartel by reducing corruption in the cartel, a tactic unlikely to have any effect other than, possibly, making the organization even more capable. Partnering with other nations to present global solutions is still possible and will likely have an effect. US-led sanctions regimes have made it harder for some nations to conduct illicit activities, and as more nations buy into these regimes, the measures become more effective. Financial targeting like the US Department of the Treasury's crackdowns on banks and front companies used by the DPRK in the mid-2000s were also effective in curbing the DPRK's SOTOC.[27] While these partnerships should still be pursued with the DPRK's trading partners, particularly China, one cannot expect these measures to have the same effect as other counter-TOC partnerships. For example, while many nations coordinated to counter cocaine trafficking by Pablo Escobar's cartel, the participation of the Colombian government was necessary to actually bring it down. Without the host nation's cooperation, the effects of global coordination will be limited, and one cannot expect the DPRK to take actions against itself. Leveraging NGOs also becomes more difficult for the same reason. Generally speaking, an NGO operates with the permission of the host government. The DPRK is already very restrictive in allowing NGOs access. NGOs seeking to combat the criminal activities of the DPRK cannot expect to be allowed entry into North Korea unless they conducted their counter-TOC activity clandestinely—a dangerous proposition. The one exception to this limitation could be NGOs operating in cyberspace, which would not require physical access to the DPRK. However, these organizations' reach would also be limited due to the DPRK's severely restricted access to the global internet.

This leaves few options for combating SOTOC like that seen in the DPRK. A traditional, supply-side–focused strategy is difficult at best when there is minimal or no access to the source country. Certainly, interdiction and confiscation outside the DPRK's borders can be tactically successful in reducing the supply and should still be used. Military interdiction in international waters remains a useful tactical tool. Further, along the supply chain, law enforcement cooperation and exchanges between willing nations, including the establishment of multinational and interagency fusion centers, should be used to increase interdiction capacity in ports

and territorial waters while also standardizing enforcement to prevent weak seams that can be exploited. This could include a more stringent version of the Container Security Initiative enacted by key destinations for DPRK shipping that increases scrutiny on those shipments. Establishing the necessary agreements for this cooperative enforcement will also require engagement in the diplomatic realm.

However, focusing on the supply side rarely leads to strategic success.[28] In that sense, combating the DPRK's SOTOC presents an opportunity. With such limited options to combat the supply side, anyone seeking to do so is forced into focusing on the demand side of the criminal activity. Strategies like reducing demand for methamphetamines and heroine in DPRK-targeted markets or promoting consumer resistance to purchasing counterfeit products could have desired effects. For counterfeit goods, an aggressive, multilateral information campaign should be used in the primary markets for DPRK's counterfeits. Strategic messaging that emphasizes negative cuing along with promoting relationship marketing by the companies whose products are being counterfeited have shown positive results.[29] For narcotics trafficking, the United States must partner with key markets for DPRK narcotics—including China, Japan, the Philippines, and Thailand—to help enact effective demand-reduction policies, including treatment programs and education.[30] These and similar tactics have been proposed academically and utilized to limited extents by the United States and other governments in their general counter-TOC strategies.[31] However, these methods must have a higher share of the overall strategy to counter the DPRK and other sources of SOTOC, if only because there is no other option.

The United States also has options in the cyber realm to directly counter state-operated cybercrime and to leverage cybertools to monitor and track other SOTOC activity. In the case of the DPRK, the United States should work to strengthen the international cybersecurity regime by promoting multilateral cybersecurity partnerships. A global regime like the 2001 Budapest Convention on Cybercrime will be hard to achieve in the near term, with key nations like China not having signed even that long-standing Convention, but more limited partnerships to specifically monitor DPRK cyberactivities could be achievable if scoped properly. The United States should conduct diplomatic engagement to explore this possibility, focusing on technically capable nations that have already been the victim of DPRK cyberactivities, while offering cybersecurity assistance to less-capable nations concerned with DPRK cyberactivities.

Finally, the area where the United States and other nations may have the most room to effectively operate is in financial targeting. The DPRK remains under strict sanctions that limit its ability to interact with global financial markets, and the United States and others have successfully frozen assets or countered financial

transfers related to DPRK organized crime. However, the DPRK has a variety of sophisticated means to evade these restrictions. The regime's money-laundering activities allow it to take full advantage of its other criminal activities and countering them could significantly reduce the effectiveness of Pyongyang's criminal enterprises. The DPRK has not only leveraged foreign banks with relatively low capabilities to counter money laundering but has also used large American banks like JPMorgan Chase and the Bank of New York Mellon, which have better capabilities against illicit transfers and present a greater opportunity for the United States to take action.[32] Pyongyang has also leveraged the burgeoning cryptocurrency market and its low level of global regulations to rapidly move money.[33]

The United States, particularly the Department of the Treasury, must continue its current trajectory of strengthening its ability to counter DPRK money laundering. This is important but insufficient by itself. The interconnectedness of the international financial system necessitates a broader approach involving global partners, particularly those with weaker anti–money-laundering capabilities or policies. The best way to do this is through what Fordham University's Seongjun Park calls "upward regulatory harmonization."[34] This policy seeks to incrementally improve anti–money-laundering capabilities among developing nations via an incentive structure, similar to some of those used to reduce carbon emissions. This appears to be more effective than a punitive approach.[35] This will likely not be a fast or complete solution, particularly since the largest regional economy, China, is hesitant to do anything that would destabilize the DPRK. Nevertheless, even partial gains in this space would be beneficial for countering DPRK SOTOC.

Conclusion

North Korea serves as the most prominent example of organized crime that is truly organized and run by a state itself. Many of the tools for analyzing and combating organized crime may not apply to this SOTOC. This presents a challenge unique from those posed by governments that are simply corrupt, complicit in, or unable to respond to organized crime. However, the recommendations offered in this article can be utilized for other states connected to TOC at a variety of levels: i.e., Venezuela, Suriname, and Russia. For those states with lower levels of government involvement, these approaches can be combined with more traditional counters to further improve overall effectiveness. The United States, along with other governments and organizations, must focus more on the demand side of the networks, while continuing to strategically engage with other key international partners and tactically engage with more traditional forms of countertrafficking like interdiction and sanctions. While such a holistic approach to countertrafficking is not a new concept, the proportional effort on each part must be

different due to the unique dynamics of SOTOC. This will be a challenge for the national security apparatus, but particularly when considering the support these activities provide to programs like the DPRK's nuclear weapons development, it must be done correctly to promote global stability.✪

Maj Brian Hill, USAF

Major Hill is an intelligence officer in the United States Air Force. He has worked in a broad range of fields, including counterterrorism, partner-nation engagement, nuclear proliferation, political-military analysis, and denial and deception. He holds a bachelor's degree in mathematics and a master's degree in intelligence studies and is pursuing a master's degree in international security with the University of Arizona.

Notes

1. Charles Tilly, "War Making and State Making as Organized Crime," in *Bringing the State Back In*, ed. Peter Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge: Cambridge University Press, 1985).

2. United Nations, "Charter of the International Military Tribunal (IMT)," in *Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis* (London Agreement), (1945); and Jens Meierhenrich, "Conspiracy in International Law," *Annual Review of Law and Social Sciences* 2 (2006): 341–57.

3. Penny Green and Tony Ward, "State Crime, Human Rights and the Limits of Criminology," *Social Justice* 27, no. 1 (Spring 2000): 101–15.

4. Douglas Farah and Kathryn Babineau, "Suriname: The New Paradigm of a Criminalized State," *Global Dispatch* 3 (March 2017), https://www.securefreesociety.org/.

5. Peter Grabosky, "Organized Cybercrime and National Security," *Information Society and Cybercrime: Challenges for Criminology and Criminal Justice*, (Seoul: Korean Institute of Criminology and International Society of Criminology Research Report Series, 2013).

6. William J. Chambliss, "State Organized Crime," *Criminology* 27 (1989), 183.

7. Alfred W. McCoy, Cathleen B. Read, and Leonard Palmer Adams, *The Politics of Heroin in Southeast Asia* (New York: Harper and Row, 1972).

8. Bahman Baktiari and Matthew C. Moen, "American Foreign Policy and the Iran-Contra Hearings," *Comparative Strategy* 7, no. 4 (1988): 427–38.

9. Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006," CSIS, June 2022, https://www.csis.org/.

10. Max Manwaring, *Gangs, Pseudo-Militaries, and Other Modern Mercenaries* (Lawton: University of Oklahoma Press, 2010).

11. Doug Farah, *Transnational Organized Crime, Terrorism, and Criminalized States in Latin America: An Emerging Tier-One National Security Priority* (Carlisle Barracks, PA: US Army War College, Strategic Studies Institute, August 2012).

12. Farah, *Transnational Organized Crime, Terrorism, and Criminalized States*.

13. Paul Rexton Kan, Bruce E. Bechtol, Jr., and Robert M. Collins, *Criminal Sovereignty: Understanding North Korea's Illicit International Activities* (Carlisle Barracks, PA: US Army War College, Strategic Studies Institute, March 2010).

14. Vincent W. Yao, "An Economic Analysis of Counterfeit Goods: The Case of China," *Business and Public Administration Studies* 1, no. 1 (2006), 116; Mark Bowden, *Killing Pablo*, (New

York: Grove Press, 2015); and Liana Sun Wyler and Dick K. Nanto, *North Korean Crime-for-Profit Activities* (Washington, DC: Congressional Research Service, 2008).

15. Raphael F. Perl, "Drug Trafficking and North Korea: Issues for US Policy," Congressional Research Service Report for Congress, 2007.

16. Zhongmin Liu, "Criminal State: Understanding Narcotics Trafficking Networks in North Korea," *Journal of Financial Crime* 26, no. 4 (2019): 1014–26.

17. US Department of State, "International Narcotics Control Strategy Report," 2015.

18. US Department of State, "International Narcotics Control Strategy Report," 2008.

19. Wyler and Nanto, *North Korean Crime-for-Profit Activities*.

20. Wyler and Nanto, *North Korean Crime-for-Profit Activities*.

21. Wyler and Nanto, *North Korean Crime-for-Profit Activities*.

22. Geoff White and Jean H. Lee, "The Lazarus Heist: How North Korea Almost Pulled Off a Billion-dollar Hack," *BBC*, 21 June 2021, https://www.bbc.com/.

23. US Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe" (public affairs release, February 2021); and Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006."

24. Bank of Korea Economic Statistics System, 2022.

25. Wyler and Nanto, *North Korean Crime-for-Profit Activities*.

26. Moisés Naím, *Illicit* (New York: Anchor, 2006).

27. Kan, Bechtol, and Collins, *Criminal Sovereignty*.

28. Naím, *Illicit*; and Tom Wainwright, *Narconomics: How to Run a Drug Cartel* (New York: Public Affairs, 2016).

29. Goutam Chakraborty, et al., "Use of Negative Cues to Reduce Demand for Counterfeit Products," *Advances in Consumer Research* 24 (1997); 345–49; and Yasmeen G. Elsantil and Eid G. Abo Hamza, "A Review of Internal and External Factors Underlying the Purchase of Counterfeit Products," *Academy of Strategic Management Journal* 20, no. 1 (2021): 1–13.

30. H. R. Sumnall, G. Bates, and L. Jones, "Evidence Review Summary: Drug Demand Reduction, Treatment and Harm Reduction," European Monitoring Centre for Drugs and Drug Addiction (commissioned background paper), 2017, https://www.drugsandalcohol.ie/; and Paul J. Turnbull and Russell Webster, "Demand Reduction Activities in the Criminal Justice System in the European Union," *Drugs: Education, Prevention and Policy* 5, no. 2 (1998); 177–84.

31. Naím, *Illicit*.

32. Andrew W. Lehren and Dan De Luce, "Secret Documents Show How North Korea Launders Money Through U.S. Banks," *NBC News*, 20 September 2020.

33. Patrick H. O'Neill, "North Korean Hackers Steal Billions in Cryptocurrency. How Do They Turn It Into Real Cash?," *MIT Technology Review*, 10 September 2020.

34. Seongjun Park, "Evading, Hacking & Laundering for Nukes: North Korea's Financial Cybercrimes & the Missing Silver Bullet for Countering Them," *Fordham International Law Journal* 45, no. 4 (March 2022): 675–716.

35. Park, "Evading, Hacking & Laundering for Nukes."