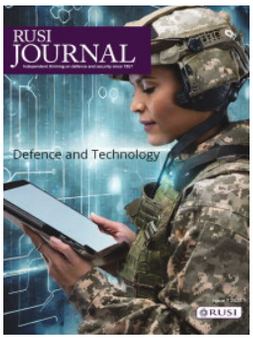


The RUSI Journal

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rusi20

Counter Threat Finance for Strategic Competition

Kevin D Stringer, Madison Urban & Andrew Mackay

To cite this article: Kevin D Stringer, Madison Urban & Andrew Mackay (2023) Counter Threat Finance for Strategic Competition, The RUSI Journal, 168:7, 42-51, DOI: 10.1080/03071847.2024.2323740

To link to this article: https://doi.org/10.1080/03071847.2024.2323740

Published online: 14 Mar 2024.

Research Article
RUSI Journal

Counter Threat Finance for Strategic Competition

Kevin D Stringer, Madison Urban and Andrew Mackay

In strategic competition, malign state and non-state actor networks pose significant threats to key national security interests. To understand and combat these networks, counter threat finance, a tool historically used to address narcotics and terrorist financing, can be applied against state actors who use money to gain influence and increase power. Kevin D Stringer, Madison Urban and Andrew Mackay argue for expanding the authority and application of counter threat finance to address state adversaries, and highlight how this is an integral element of a nascent whole-of-nation economic statecraft strategy and an essential step towards gaining the edge in strategic competition.

Outside its community of practitioners, counter threat finance (CTF) is a little-understood national security instrument. However, as one author noted, '[f]inancing is the lifeblood of all organizations, and its interdiction or disruption can impair the ability of any entity to operate effectively'.[1] Emerging from the counternarcotics and counterterrorism worlds, CTF has significant value and application in strategic competition against state adversaries, particularly China, Russia, Iran and North Korea. When integrated into a broader national security strategy and hybrid warfare campaign, CTF is an important tool that can be used to proactively shape contested environments, improve geopolitical and geoeconomic positions, and mitigate commercial and economic vulnerabilities from hybrid threats – a term used synonymously with irregular warfare activities. Finance is central to network operations, and CTF is a critical part of disrupting threat networks.

While the US and its partners primarily use CTF to target illicit non-state actors, it warrants greater adaptation to adversarial countries. In today's global threat environment, CTF ought to be used against state adversaries that use both licit and illicit financial levers to shape, influence and control relevant populations, revenue streams, state and local governments, officials and supply chains. This article focuses on the US, and particularly the US Department of Defense (DoD) as a starting point, but future, planned research will consider the broader US interagency as well as allies' and adversaries' approaches to the topic – which is necessary to account for the various government siloes that confront threat finance. This article defines CTF, characterises its activities, situates it in the context of economic warfare, financial warfare, and anti-money laundering, and then offers a preliminary framework for its application against state actors. The conclusion proffers lines of study for further research as well as illustrates how CTF might best nest under a broader, whole-of-nation economic statecraft strategy.

Methodology

The methodological approach for this research essay consisted of a series of semi-structured interviews combined with the review and use of a broad range of secondary literature on threat finance. For the former, the authors conducted five small group interviews in Spring 2023 with active

1. Kevin D Stringer, 'Counter Threat Finance (CTF): Grasping the Eel', *Military Power Revue* (No. 2, 2013), pp. 64–70.

Counter threat finance could be used to tackle the activities of malign states. *Courtesy of monticellllo / Adobe Stock*

CTF experts and practitioners from the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S), the Office of the Deputy Assistant Secretary of Defense for Counternarcotics and Stabilization Policy (OASD CNSP), US Special Operations Command, US Central Command, US Indo-Pacific Command and the US Defense Intelligence Agency. The interviewees are all considered experts by the DoD CTF community, and their respective organisational placements provide a satisfactory overview and depth to the CTF topic from both a strategic and operational level. The discussions sought to understand the DoD's current authorities, existing interagency cooperation, the level of CTF professionalisation and training, and insights into how to improve current capabilities, processes and structures. The authors asked the interviewees about their perspectives on the role and utility of CTF in strategic competition against peer and near-peer adversaries, the best placement of this function for strategic competition within government, and any recommended changes to organisational or conceptual approaches.

The authors also surveyed the significant body of existing works on threat finance. While this literature base is large, most scholarly articles concentrate on terrorist or criminal financing, or the convergence thereof, and only tangentially touch state actors.[2]

2. See, for example, Kevin D Stringer, 'Tackling Threat Finance: A Labor for Hercules or Sisyphus?', *Parameters* (Vol. 41, No. 1, 2011), p. 101; Shima D Keene, *Threat Finance: Disconnecting the Lifeline of Organised Crime and Terrorism* (Abingdon: Routledge, 2016); David Blum et al. (eds), *Counterterrorism and Threat Finance Analysis During Wartime* (Lanham, MD: Lexington Books, 2015); Michael Miklaucic and Jacqueline Brewer (eds), *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington, DC: Center for Complex Operations, NDU, 2013); Jeremy Kuester, 'Transnational Influences on Financial Crime', *Miami National Security and Armed Conflict Law Review* 71 (Vol. 4, No. 2, 2014); Danielle Cammer Lindholm and Celina B Realuyo, 'Threat Finance: A Critical Enabler for Illicit Networks', in Miklaucic and Brewer (eds), *Convergence*; J Edward Conway, 'Analysis in Combat: The Deployed Threat Finance Analyst', *Small Wars Journal*, 4 July 2012, <www.smallwarsjournal.com/jrnl>, accessed 17 January 2024; Michael Levi, 'Combating the Financing of Terrorism: A History and Assessment of the Control of "Threat Finance"', *British Journal of Criminology* (Vol. 50, No. 4, 2010), pp. 650–69; Michael Jacobson and Matthew Levitt, 'Combating the Financing of Transnational Threats', Emirates Center for Strategic Studies and Research (ECSSR), 2009; and Thomas R Cook, 'The Financial Arm of the FARC: A Threat Finance Perspective', *Journal of Strategic Security* (Vol. 4, No. 1, March 2011), pp. 19–36.

DOI: 10.1080/03071847.2024.2323740

Second, the authors align with Thomas Biersteker, who in 2011 provided an important critique of current threat finance literature and the so-called 'experts' who produce it.[3] In essence, Biersteker assessed that:

> Given the relative paucity of reliable information on the financing of terrorism and the complex nature of the phenomenon, numerous authors have produced a vast literature on the subject. Most of the published work is highly repetitive, with a frequent restatement of highly stylized facts and broad generalizations. While these works might be good for producing catchy headlines, their analytical basis generally leaves much to be desired, and the focus on a single dimension or source of financing terrorism is reductionist and trivializes the complexity of the subject. The literature is better on the regulatory regime and policy-side than on the analysis of the actual financing of terrorism. This is logical since it is easier to access government and intergovernmental policy practitioners than individuals who engage in real acts of terrorism.[4]

While the US and its partners primarily use CTF to target illicit non-state actors, it warrants greater adaptation to adversarial countries

As such, the authors aimed to extract only the elements that were relevant for the use of CTF in state power competition, while complementing it with both policy and operational practitioner knowledge derived from the interviews and the authors' own backgrounds.[5] The article acknowledges the blurriness between state and non-state power interfaces in this field, and concurs with Jessica Davis' analysis that CTF approaches, at least as applied in the counterterrorism space, remain poorly understood in terms of effects and outcomes.[6] Hence, this article aims to initiate thinking on CTF concepts that can apply to state actors, who will likely manifest slightly different financing behaviours and profiles than terrorist groups.

Definitions of Counter Threat Finance

While there is no singular definition of CTF in the US or partner nations, the DoD defines counter threat finance as a broad range of 'activities conducted to deny, disrupt, destroy, or defeat the generation, storage, movement, and use of assets to fund activities that support an adversary's ability to negatively affect United States interests'.[7] There are two main components of CTF: threat finance intelligence (TFI) and counter threat finance operations (CTFO). TFI is the collection of relevant adversarial financial information and subsequent analysis of how the money is generated, moved, stored and used. CTFO refers to actions against malign activity, both witting and unwitting – examples include arrest, surveillance, sanctioning and asset seizure. At times, merely understanding an adversary's financial flows offers valuable insights into its operations, strategic directions, potential centres of gravity, and vulnerabilities.

CTF actions derive from specific authorities and capabilities that exist across US agencies, as well as international partners and allies. Yet, there are limitations. For example, while the DoD can be a contributory partner, it often does not have the authorisation to operate directly against a malign actor and must rely upon the legal prerogatives of other US departments or partner nations. These entities include US law enforcement agencies (for example, Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Customs and Border Protection (CBP), Homeland Security Investigations (HSI)) and departments with sanction authorities (such as the Department of State (DoS), Department of the Treasury (USDT), Department of Commerce (DOC)). Despite differences in terminology and definitions, each organisation

3. Stringer, 'Counter Threat Finance', pp. 64–70.
4. Thomas J Biersteker, 'Trends in Terrorist Financing – A Review of the Literature, Report Prepared for Booz, Allen, & Hamilton Consultants', Washington, DC, August 2011.
5. The authors have collectively special operations, intelligence and research backgrounds that have been applied to CTF initiatives and environments. Two of the authors also have banking sector experience in anti-money laundering activities.
6. Jessica Davis, 'Understanding the Effects and Impacts of Counter-Terrorist Financing Policy and Practice', *Terrorism and Political Violence* (Vol. 36, No. 1, 2024), pp. 1–17.
7. US Department of Defense (DoD), *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02, as of November 2021, <https://irp.fas.org/doddir/dod/dictionary.pdf>, accessed 17 January 2024.

possesses unique operational permissions to deny, disrupt, destroy and defeat malign financial networks. These permissions can also be layered to achieve a broader effect.[8]

Distinguishing CTF from Economic and Financial Warfare

Before fleshing out the possible uses of CTF in the current competitive environment, it is necessary to situate CTF in the context of economic warfare, financial warfare, and anti-money laundering, countering the financing of terrorism, and counter-proliferation financing (AML/CFT/CPF) efforts. To effectively segment these activities, it is essential to understand the difference between the economy and finance. Economics relates to the production and consumption of goods and services in a society involving capital, resources and labour and economic warfare has been defined as 'the conscious attempt to enhance the relative economic, military, and political position of a country through foreign economic relations'.[9] The tools of economic warfare include blockades, embargoes, preclusive buying, state trading and coercive use of an imbalance of economic power.[10] Economic warfare has been part of conflict for millennia, dating back to the first known example of sanctions and trade embargoes with the Megarian Decree in the Peloponnesian War in the 430s BCE.[11] However, an economy is created through the exchange of money and use of credit, the movement of which is the study of finance, and as such, the weaponisation of finance is a subset of economic warfare.[12]

Financial warfare aims to undermine the monetary foundations of an adversary or disrupt particular transactions, both of which can also have broader economic impacts.[13] The modus and intensity of financial warfare changed considerably following 9/11, when former USDT Undersecretary for Enforcement Jimmy Gurule spoke of 'waging a financial war' to 'financially paralyze and marginalize those who serve as financial supporters and intermediaries for terrorists'.[14] In the context of this financial warfare against terrorist actors, CTF became a key method for dismantling threat networks overseas. At the operational level, the DEA-headed Afghan Threat Finance Cell (ATFC) and the Iraq Threat Finance Cell (ITFC), co-led by DoD and USDT, proved the utility of CTF, successfully targeting and disrupting insurgents' financial networks and individual financiers.[15] The ATFC efforts to counter terrorist funding and narcotics trafficking also exposed Afghan corruption in support of broader stabilisation and democratisation efforts.[16] Various national security agencies supported the cells, giving them additional capabilities and access into a variety of forms of intelligence, including signals intelligence, human intelligence, geo-spatial intelligence, and documentary exploitation.[17] The techniques used by the IFTC and AFTC, such as social network analysis (SNA), influence network modelling (INM), multi-objective decision analysis (MODA) and course of action (COA) development, are relevant beyond the counter-insurgency (COIN), counterterrorism and counternarcotics environments.[18] However, the

8. US DoD, 'DoD Counter Threat Finance (CTF) Policy, DoD Directive 5205.14, as of May 3, 2017', <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520514p.pdf?ver=2019-02-05-084012-033>, accessed 11 January 2024; Trevor Johnston et al., *Countering Violent Nonstate Actor Financing: Revenue Sources, Financing Strategies, and Tools of Disruption* (Santa Monica, CA: RAND, 2023) pp. 106–14.
9. Robert Loring Allen, 'State Trading and Economic Warfare', *Law and Contemporary Problems* (Vol. 24, Spring, 1959), p. 259, <https://scholarship.law.duke.edu/lcp/vol24/iss2/3>, accessed 11 January 2024.
10. Charles Cortez Abbott, 'Economic Warfare - The Attack', *Naval War College Review* (Vol. 2, No. 2, Article 3, 1949), <https://digital-commons.usnwc.edu/nwc-review/vol2/iss2/3>, accessed 14 January 2024; David J Katz, 'Waging Financial Warfare: Why and How', *Parameters* (Vol. 47, No. 2, 2017), p. 42.
11. PA Brunt, 'The Megarian Decree', *Studies in Greek History and Thought* (Oxford, 1992: online edn, Oxford Academic, 2023).
12. Katz, 'Waging Financial Warfare'.
13. *Ibid*.
14. Jimmy Gurule, 'September 11, 2001: Attack on America', Speech before the American Bankers Association Money Laundering Conference, Arlington, Virginia, 22 October 2001, <http://avalon.law.yale.edu/sept11/treas_012.asp>, accessed 6 January 2024.
15. Lindholm and Realuyo, 'Threat Finance', p. 122; Johnston et al., *Countering Violent Nonstate Actor Financing*.
16. Lindholm and Realuyo, 'Threat Finance', p. 122.
17. Conway, 'Analysis in Combat'.
18. David M Blum and J Edward Conway (eds), *Counterterrorism and Threat Finance Analysis During Wartime* (Lanham, MD: Lexington Books, 2015).

financial warfare model that solidified during decades of counter-terrorism efforts did not solely rely on state power but also leveraged the private sector through the Financial Action Task Force's (FATF) AML/CFT/CPF regimes.

The FATF, an intergovernmental organisation founded in 1989, 'leads global action to tackle money laundering, terrorist and proliferation financing, and ... promotes global standards to mitigate the risks, and assesses whether countries are taking effective action'.[19] The FATF oversees the global AML/CFT/CPF architecture. While it lacks enforcement capabilities, its ability to grey-list or black-list jurisdictions that fail to comply with its standards can have a significant negative impact on non-compliant financial sectors and the respective national GDP.[20] As most of FATF's recommendations are codified in US legislation, domestic law enforcement agencies often interdict threat finance by using AML/CFT/CPF rules to deny, disrupt, destroy, and defeat malign financial networks.[21] While there are similarities and overlaps between CTF and AML/CFT/CPF in the financial data, technology, processes, skills and capabilities domains, they are not synonymous.

International partners similarly emphasise the importance of CTF in the current competitive environment. For instance, the UK Ministry of Defence recently published a Joint Doctrine Note on Threat Finance and the Economic Levers of Power (JDN 2/20), outlining the applicability of TFI and CTFO to oppose hybrid threats in conjunction with other departments and agencies.[22] The document also underscores that finance 'can be a tool of diplomacy; but it can also be equally used as a tool of security and war' and outlines the wide range of tactical and strategic benefits of understanding and countering financial networks.[23] While JDN 2/20 focuses extensively on countering illicit activities, there are equal benefits to understanding, influencing, and acting against legal, albeit malign state networks.

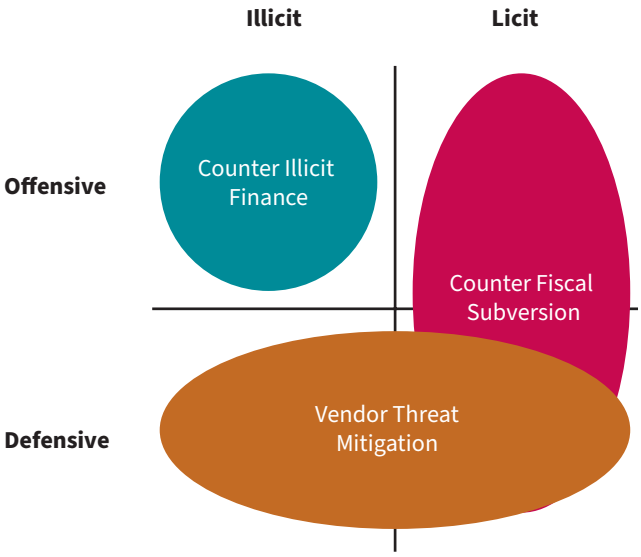
CTF Framework: Licit and Illicit Finance, Defensive and Offensive Activities

In the context of strategic competition, CTF must concentrate on both the traditional illicit organisations, such as drug trafficking organisations, terrorist groups and transnational criminal organisations, as well as the licit networks involved in foreign direct investment, debt financing and company acquisition. For example, the People's Republic of China's (PRC) legal economic investment in a country can make the recipient more acquiescent to Chinese interests or turn individual national lawmakers into PRC advocates to gain pecuniary advantages for their local districts. Correspondingly, the PRC could also interfere with operations at a US military base by manipulating permissible investments in critical infrastructure (for instance, electric grids or ports).

For both licit and illicit activities, CTF delivers both defensive and offensive capabilities. For the former, the goal is to identify and deny avenues through which adversarial financial networks could exploit DoD vulnerabilities. For the latter, the objective is to target the weaknesses of adversarial state financial networks and impose costs. The combination of offensive and defensive actions against licit and illicit networks produces at least three distinct conceptual methods where CTF can be implemented: tackling illicit finance; providing vendor threat mitigation; and opposing fiscal subversion (see Figure 1). These areas serve as a framework and categorisation for conceptualising and implementing CTF operations and activities. They also serve to take existing but disparate threat finance themes from counterterrorism and counternarcotics and organise them in a logical way for application against state actors.

19. Financial Action Task Force, 'What We Do', <https://www.fatf-gafi.org/en/the-fatf/what-we-do.html>, accessed 10 January 2024.
20. *Ibid*.
21. FATF, 'Anti-money Laundering and Counter-terrorist Financing Measures: United States, 3rd Enhanced Follow-up Report and Technical Compliance Re-Rating', 31 March 2020, <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur-united-states-2020.html>, accessed 10 January 2024; Special Inspector General for Afghanistan Reconstruction, 'Counter Threat Finance: U.S. Agencies Do Not Know the Full Cost and Impact of Their Efforts to Disrupt Illicit Narcotics Financing in Afghanistan', March 2021, p. 22, <https://www.sigar.mil/pdf/audits/SIGAR-21-29-AR.pdf>, accessed 14 January 2024.
22. MoD, 'Threat Finance and the Economic Levers of Power', Joint Doctrine Note 2/20, November 2020, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/937149/20201119-JDN_2_20_TFEL_web_secure.pdf>, accessed 10 January 2024.
23. *Ibid.*

Figure 1: Counter Threat Finance Vectors



Source: The authors.

Countering Illicit Finance: Crime-State Nexus

Impeding illicit finance is the traditional role of CTF against non-state actors (such as drug cartels, terrorist groups and transnational criminal organisations) as well as states that use these proxies to engage in other illicit activity (for instance, bribery or corruption) in ways that harm national interests. The placement of CTF authorities and funding within the DoD reflects this legacy role. The primary authority for these CTF activities derives from 10 USC §284, the section on 'support for counterdrug activities and activities to counter transnational organized crime', with funding oversight residing with the Office of the Deputy Assistant Secretary of Defense for Counternarcotics and Stabilization Policy (DASD(CN&SP)). While counternarcotics is not the ideal placement of authorities and monies for dealing with state actors, the current arrangement does permit significant emphasis on the state financiers of terrorism and directed crime. Examples of the former include Iran and Syria and their respective proxies.[24] Iran remains 'the leading state sponsor of terrorism, facilitating a wide range of terrorist and other illicit activities around the world' including 'large-scale illicit financing schemes and money laundering to fund its malign activities'.[25] The current CTF legal framework still provides the ability to address such a threat.

On the crime-state actor nexus, the CTF transnational organised crime permissions allow action against Chinese state activity. A pertinent example is the complicity of the Chinese Communist Party (CCP) as a state sponsor of criminal activities for the trafficking of fentanyl precursor chemicals to Mexican cartels. On 23 June 2023, the US Department of Justice announced the first arrests and indictments of Chinese nationals and China-based manufacturing companies for their role in supplying Mexican cartels with fentanyl precursor chemicals. Fentanyl is now the leading cause of death for individuals aged 18 to 49 in the US and 'fentanyl-related precursors are principally sourced from China-based chemical manufacturers'.[26] The export of these Chinese precursor substances is a hybrid warfare line of effort directed against the US, and since the underlying commercial business requires funding, CTF tactics, techniques and procedures can support law enforcement operations, activities and actions that disrupt this drug flow. As Deputy Attorney General Lisa O Monaco stated, 'The Justice Department will not rest or relent in investigating and prosecuting every link of the fentanyl supply chain, including the PRC companies and executives who produce and export vast quantities of the precursor chemicals the drug cartels need to peddle their poison. There can be no safe haven'.[27]

Russia also uses transnational criminal organisations to access funding and transfer capital when suitable. In 2022, as the West began to isolate Moscow economically in the wake of the invasion of Ukraine, Kristian Vanderwaeren, the head of the Belgian General Administration of Customs and Excise, noted that 'by midyear, we had seen

24. US Department of the Treasury, 'National Strategy for Combating Terrorist and Other Illicit Financing', Washington, DC, 2018, <https://home.treasury.gov/system/files/136/nationalstrategyforcombatingterroristandotherillicitfinancing.pdf>, accessed 14 January 2024.
25. US Department of State, 'Country Reports on Terrorism 2021', 27 February 2023, <https://www.state.gov/reports/country-reports-on-terrorism-2021/>, accessed 14 January 2024.
26. Indictment, *United States of America v. Hubei Amarvel Biotech Co., LTD.*, Docket No. 1:23-cr-00302 (S.D.N.Y. Jun 22, 2023), <https://www.justice.gov/media/1301721/dl?inline>, accessed 11 January 2024.
27. US Department of Justice, 'Justice Department Announces Charges Against China-Based Chemical Manufacturing Companies and Arrests of Executives in Fentanyl Manufacturing', press release, 23 June 2023, <https://www.justice.gov/opa/pr/justice-department-announces-charges-against-china-based-chemical-manufacturing-companies>, accessed 14 January 2024.

a massive increase in traditional illegal activity from Russian-linked groups that appear to have Russian government backing working to develop new revenue streams to replace damage from the sanctions'.[28] Western governments also suspect that Russian intelligence agencies have links to the recently freed arms trafficker, Victor Bout, who circumvented arms embargoes around the world and funnelled weapons to groups opposed by the US, including an attempt to procure weapons for the Revolutionary Armed Forces of Colombia-People's Army (FARC).[29] After his 2008 arrest in Thailand, a US federal court convicted Bout of 'conspiracy to support terrorists, conspiracy to kill Americans, and money laundering'.[30] Each of these charges fundamentally relates to the movement of goods and money that could have been tracked and interdicted through CTF actions.[31]

The PRC and Russia also exploit bribery and corruption to achieve strategic ends. The World Bank has sanctioned a multitude of Chinese companies, including Chinese state-owned entities and their subsidiaries, for a variety of fraudulent business practices. A China-based firm, Zhejiang First Hydro, was disbarred in 2021 after it 'offered and paid bribes to two government officials in exchange for a contract'.[32] Both Bangladesh and Bolivia, in 2018 and 2022 respectively, accused the China Harbor Engineering Company, a subsidiary of a state-owned entity, of bribery.[33] The Kremlin also strategically leverages corruption to expand its global footprint and uses a variety of means to evade sanctions.[34]

All these activities have a funding dimension that current CTF capabilities can target. Finance is at the heart of malign organisations' ability to achieve effects, whether it be to purchase necessary equipment, pay its members or employees, or bribe decision-makers. Thus, TFI can illuminate adversarial flows of money and provide insights into the true intentions of a state actor, and then a range of authorities can be exercised in CTFO to minimise the impact of, or terminate, the malign activity.

Vendor Threat Mitigation: Defensive, Licit and Illicit

The second type of CTF is vendor threat mitigation (VTM), an inherently defensive vector of CTF. These measures aim to 'identify and address threats posed by vendors that oppose US, allies', or partners' interests or pose a threat to national security'.[35] Given the US' massive reliance on contracted support for operations overseas, VTM seeks to protect DoD money and information by ensuring contractors that support military operations do not have connections with nefarious state or non-state actors. Using both financial and non-financial indicators, VTM provides a defensive framework for identifying malign actors and managing the risk of using contracted support and commercially developed technology solutions acquired for DoD operations globally. VTM leverages a variety of authorities – acquisition, counter threat finance, force protection, intelligence and law enforcement – to manage risk and deny adversaries access to information (including intellectual capital

28. Mitchell Prothero, 'Russian Spies Have Gone Full Mafia Mode Because of Ukraine', *Vice*, 27 October 2022.
29. United Nations Office on Drugs and Crime (UNODC), Case Law database, 'United States vs Viktor Bout', <https://sherloc.unodc.org/cld/case-law-doc/criminalgroupcrimetype/usa/2013/united_states_v_viktor_bout.html?lng=en&tmpl=sherloc>, accessed 10 February 2024.
30. *Ibid*.
31. Felix Light, 'Explainer: Who is Viktor Bout, Arms Dealer Linked to Swap for Americans Held by Russia?', *Reuters*, 5 August 2022.
32. World Bank, 'World Bank Group Debars Zhejiang First Hydro & Power Construction Group Co.', press release, 16 June 2021, <https://www.worldbank.org/en/news/press-release/2021/06/16/world-bank-group-debars-zhejiang-first-hydro-power-construction-group-co>, accessed 14 January 2024.
33. *Agence France-Presse*, 'Bangladesh Blacklists Chinese Construction Firm, Cancels Highway Deal after Bribe Claim', *South China Morning Post*, 18 January 2018; Luis Marcelo Tedesqui Vargas, 'Fiscalía Dice que Zhengyuan "Lavó" el Dinero de la Supuesta Coima a la ABC y lo Recaptura' ['Prosecutor's Office Says that Zhengyuan "Laundered" the Money from the Alleged Bribe to ABC and Recaptured It'], *El Deber* (Bolivia), 16 September 2022, <https://eldeber.com.bo/pais/fiscalia-dice-que-zhengyuan-lavo-el-dinero-de-la-supuesta-coima-a-la-abc-y-lo-recaptura_293148>, accessed 10 January 2024.
34. Philip Zelikow et al., 'The Rise of Strategic Corruption: How States Weaponize Graft', *Foreign Affairs*, 9 June 2020; Tom Collins, 'How Putin Prepared for Sanctions with Tonnes of African Gold', *The Telegraph*, 3 March 2022; US Department of the Treasury, 'Russian Elites, Proxies, and Oligarchs Task Force', Global Advisory on Russian Sanctions Evasion Issued Jointly by the Multilateral REPO Task Force, 9 March 2023, <https://home.treasury.gov/system/files/136/REPO_Joint_Advisory.pdf>, accessed 10 January 2024.
35. US DoD, 'Vendor Threat Mitigation', DoD Directive 3000.16, 6 July 2022, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300016p.PDF?ver=DeK4wPD-OT_ihFTwQXHyzA%3D%3D>, accessed 10 January 2024.

and intelligence), money and other goods (for example, military technology). Ultimately, VTM seeks to understand the range of commercial threats to both deny opportunities for exploitation and impose costs.[36]

Historically, public awareness and consolidation of VTM efforts began in earnest after contracting mishaps funnelled DoD money and goods to US enemies in Afghanistan. In 2011, the Afghanistan Host Nation Trucking Contract caused a public scandal when it became known that several of the eight DoD contracted entities to transport goods across Afghanistan to US troops had funnelled some $700 million to Taliban insurgents and local warlords through a system of subcontracts.[37] After a Pentagon investigation, a Congressional hearing, and an excoriating House subcommittee report, the US government enacted a series of reforms.[38] The VTM sub-element of CTF emerged from this context.

In the context of strategic competition, particularly as PRC manufacturing wins greater market share in critical technologies, VTM efforts extend beyond the counterterrorism and counter-insurgency context. As private companies in the PRC can be legally required to provide information or conduct espionage on behalf of the Chinese government, there are significant concerns about the use of PRC manufactured technologies that could collect intelligence in US government and military work.[39] There are additional concerns about how the procurement of PRC technologies could be used to introduce malware into sensitive or critical systems, as exemplified by the December 2023 letter by US senators criticising the use of PRC-manufactured batteries at US Marine Corps base Camp Lejune; this letter caused the local power manufacturer to disconnect the power supply due to justified security concerns.[40] As PRC manufactured components and technologies proliferate domestically and internationally, the VTM community moves to the forefront of the threat finance, cybersecurity and counterintelligence nexus.

Countering Fiscal Subversion

Finally, CTF can also be applied to survey the fiscal 'terrain' of contested zones and potential future battlefields to inform strategic decision-makers and campaign planners.[41] For instance, US forces can scout and prepare the financial battlefield just like the physical one, and CTF can be the starting point to uncover and disrupt an adversary's monetary networks (see Figure 2 for the types of questions that could be asked about relevant financial terrain using the US Army's OCOKA factors as a model).[42] Although OCOKA is a tactical tool, its principles can be applied to an operational/strategic instrument like CTF to understand opponent fiscal networks and provide insight into potential vulnerabilities in operational plans (for example, a port's reliance on an electric grid where a Chinese company is the majority owner) or likely targets of disinformation or bribery. These insights can form the foundation of a strategy to counter that influence, using the range of authorities and capabilities available to the US government and its partners and allies.

36. Authors interview with DoD CTF representative, via email, 22 May 2023.
37. Subcommittee on National Security and Foreign Affairs of the House Committee on Oversight and Government Reform, 'Warlord Inc.: Extortion and Corruption Along the U.S. Supply Chain in Afghanistan', 22 June 2010, <https://www.cbsnews.com/htdocs/pdf/HNT_Report.pdf>, accessed 17 January 2024; US Library of Congress, Congressional Research Service, *Wartime Contracting in Afghanistan: Analysis and Issues for Congress*, R42084, 14 November 2011.
38. Subcommittee on National Security and Foreign Affairs of the House Committee on Oversight and Government Reform, 'Warlord Inc'.
39. John F Troxell, 'Geoeconomics', *Military Review* (January–February 2018), pp. 6, 11, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2018/Geoeconomics/>, accessed 17 January 2024; Scott Kennedy and Ilaria Mazzocco, 'Can Chinese Firms Be Truly Private?', Center for Strategic and International Studies, 7 February 2023, <https://bigdatachina.csis.org/can-chinese-firms-be-truly-private/#:~:text=The%20vast%20majority%20of%20firms,enterprises%20(see%20Figure%201)>, accessed 17 January 2024.
40. Marco Rubio, 'Rubio, Colleagues Warn of Communist China-Linked Batteries at U.S. Military Bases', press release, 1 December 2023, <https://www.rubio.senate.gov/rubio-colleagues-warn-of-communist-china-linked-batteries-at-u-s-military-bases/#:~:text=This%20past%20spring%2C%20CATL%20batteries,CATL%20batteries%20at%20Camp%20Lejeune.>, accessed 17 January 2024; Michael Martina, 'Duke Energy Disconnects CATL Batteries from Marine Corps Base Over Security Concerns', *Reuters*, 7 December 2023.
41. Sara Dudley, Kevin D Stringer, Steve Ferenzi, 'Beyond Direct Action: A Counter-Threat Finance Approach to Competition', *Insights* (Vol. 1, Issue 3), The KCIS, April 2021, <https://www.thekcis.org/publications/insight-13>, accessed 16 January 2024.
42. Authors video interview with DoD CTF expert, 11 May 2023.

Figure 2: Sample OCOKA Questions Applied to CTF

Observation and Fields of Fire. What things must an adversary be able to observe in order to effectively transfer value within a specific area?

Cover and Concealement. How will the adversary have to obfuscate how they transfer value?

Obstacles. What obstacles exist for an adversarial network to transfer value?

Key Terrain. What key terrain must an adversarial network have in order to transfer value?

Avenues of Approach. What are the ways in which an adversary will transfer value within a specific area?

Source: The authors. Derived from an INDOPACOM video interview with follow-up email, Spring 2023.

As the PRC and Russia expand their influence through economic investment, the CTF vector of countering fiscal subversion is becoming increasingly important. For its part, Russia props up friendly governments through security contracts, ostensibly to perform counterterrorism, training or protection missions. In exchange, Russia gains access to gold, oil and minerals – valuable assets to avoid Western sanctions.[43] Equally, the CCP's Belt and Road initiative promises billions, if not trillions, of dollars of investment in infrastructure projects around the world.[44] In particular, the PRC has co-opted key nations in the global South to gain access to strategic territory – the PRC's first permanent overseas base in Djibouti was accompanied by significant increases in investment and economic cooperation – and to control key natural resources.[45] Moreover, as Western countries seek to develop sustainable energy technologies that rely on rare earth minerals, the PRC's control of such elements or their refining process in the key source countries gives Beijing a strategic advantage over the West.[46]

While the prospect of economic development can make entire countries more acquiescent to the PRC, the CCP has also subverted local officials to advance Chinese interests in the context of their own political system. For example, in the province of Cagayan, on the northern tip of the Philippines' primary island Luzon and close to Taiwan, China signed deals and proposed development opportunities worth up to $12.2 billion.[47] While some of the anticipated contracts fell through due to the Filipino government's security concerns, the local governor, Manuel Mamba, publicly called for greater investment and ties with the PRC, not the US. 'I'm really pro-China', Mamba said. 'What will I do with America? This is the one that will invest in us. They're the ones interested in us'.[48] Despite Mamba's advocacy against US presence, the US will add two new bases in Cagayan – in line with the expansion of the US–Philippines Enhanced Defense Cooperation Agreement.[49] In this case, the federal government's relationship with the US and security

43. Daveed Gartenstein-Ross, Emelie Chace-Donahue and Colin Clarke, 'Understanding the US Designation of the Wagner Group as a Transnational Criminal Organisation', ICCT, 25 January 2023, <https://www.icct.nl/publication/understanding-us-designation-wagner-group-transnational-criminal-organisation>, accessed 17 January 2024.
44. James McBride, Noah Berman and Andrew Chatzky, 'China's Massive Belt and Road Initiative', Council on Foreign Relations, <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative>, accessed 24 May 2023.
45. IMF, 'Djibouti: 2016 Article IV Consultation-Press Release; Staff Report; and Statement by the Executive Director for Djibouti', IMF Country Report No. 17/87 (Washington, DC: International Monetary Fund, April 2017), <https://www.imf.org/-/media/Files/Publications/CR/2017/cr1787.ashx>, accessed 10 January 2024; Morgan D Bazilian, Emily J Holland and Joshua Busby, 'America's Military Depends on Minerals That China Controls', *Foreign Policy*, 16 March 2023.
46. Bazilian, Holland and Busby, 'America's Military Depends on Minerals That China Controls'; Robert Johnston, 'Supply of Critical Minerals Amid the Russia-Ukraine War and Possible Sanctions', Center on Global Energy Policy, 19 April 2022, <https://www.energypolicy.columbia.edu/publications/supply-critical-minerals-amid-russia-ukraine-war-and-possible-sanctions/>, accessed 17 January 2024.
47. Melissa Luz Lopez, 'Chinese Firms Interested in Cagayan', CNN (Philippines), 20 April 2019, <https://www.cnnphilippines.com/business/2019/4/30/Lopez-Cagayan-interest-.html>, accessed 10 January 2024.
48. Frances Mangosing, 'Pro-China Governor Opposes PH-US Live-fire Drills', *Inquirer* (Philippines), 13 January 2022, <https://newsinfo.inquirer.net/1539757/pro-china-gov-opposes-ph-us-live-fire-drills>, accessed 10 January 2024.
49. Frances Mangosing, 'Cagayan Governor Seeks Stronger Ties with Beijing', *Inquirer* (Philippines), 29 May 2023, <https://newsinfo.inquirer.net/1776034/cagayan-governor-seeks-stronger-ties-with-beijing/amp>, accessed 10 January 2024.

concerns trumped a local official. Yet, the PRC use of commerce at the local level to attempt to subvert Filipino federal interests is clear. Furthermore, the CCP might try to manipulate the local government to degrade or disrupt US military installations or operations in the future. Without an understanding of where and how money is flowing to different local or regional actors, it is difficult to understand these risks before it is too late. Fiscal subversion, because it is legal as noted by the above examples, may be mostly a TFI effort with more creative thinking needed to understand what sort of countering operations might be applicable or even possible. Some options range from strategic communication or influence operations through to capacity building and humanitarian aid programmes.

The Importance of CTF for Strategic Competition and Hybrid Threats

Whether licit or illicit, money generates influence and is the lifeblood of any organisation or network. Given its centrality to the current strategic competition, building strategies to counter malign state fiscal activity is critical. Each framework line of effort – be it counter illicit finance, vendor threat mitigation, or counter fiscal subversion – has a role in irregular competition, where the primary contest is influence over relevant populations, commercial enterprises and municipal/state officials. State-enabled non-state actors, including transnational criminal organisations, terrorist entities and cartels, continue to pose a threat to US and Allied security interests and personnel. State actors, primarily China and Russia, are increasingly buying influence over natural resources and territory while providing financial assistance and investment for political favours at the expense of the US and its allies. As the 2023 NATO Vilnius communique stated, 'The PRC seeks to control key technological and industrial sectors, critical infrastructure, and strategic materials and supply chains. It uses its economic leverage to create strategic dependencies and enhance its influence. It strives to subvert the rules-based international order, including in the space, cyber and maritime domains'.[50] This economic thrust needs financial flows to achieve its objectives.

The world's financial landscape is constantly evolving and shifting. As adversarial networks grow in size and influence, mapping the financial systems that state and non-state competitors use provides a foundation for forecasting and navigating the strategic competition space. The CTF toolkit already exists to combat these malign networks, but the authorities and mission sets need to expand and adapt, and the education of CTF practitioners needs to improve. Both these steps would also account for the need to align the multiple government siloes that are currently involved in the topic. With this in mind, topical areas for future CTF dialogue, analysis and research include: resourcing CTF as a primary strategic competition line of effort for irregular and hybrid warfare; promulgating financial intelligence as its own discipline (including for government civilians); establishing a clear career path with successive levels of education for the CTF professional; and for the DoD, assigning a military service ownership of the CTF function. Ultimately, counter threat finance is an integral element of a nascent whole-of-nation economic statecraft strategy – an essential step towards gaining the edge in strategic competition. ■

Kevin D Stringer, Colonel, US Army (Retired), is a chair for the US Irregular Warfare Center, visiting faculty at the Military Academy of Lithuania, and a lecturer at the University of Northwestern Switzerland. With 30 years of commissioned military service, he was a foreign area officer assigned to the US special operations community.

Madison Urban is an Analyst II at Valens Global and an Analyst at the Irregular Warfare Center with a research focus on strategic competition, non-state actors and economic statecraft.

Andrew Mackay is a former Royal Navy intelligence officer specialising in threat finance, former complex financial crime investigator for a global bank, Associate Fellow at RUSI CFCS and PhD candidate at the United Nations University, focused on illicit finance.

50. NATO, 'Vilnius Summit Communiqué', press release, 11 July 2023, <https://www.nato.int/cps/en/natohq/official_texts_217320.htm>, accessed 17 January 2024.