APRIL 2022

Strategic Competition in the Financial Gray Zone

AUTHORS

Heather A. Conley

James A. Lewis

Eugenia Lostri

Donatienne Ruy

A Report of the CSIS Europe, Russia, and Eurasia Program and Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2022

Strategic Competition in the Financial Gray Zone

AUTHORS
Heather A. Conley
James A. Lewis
Eugenia Lostri
Donatienne Ruy

A Report of the CSIS Europe, Russia, and Eurasia Program and Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

We are deeply indebted to CSIS senior adviser and chairman and cofounder of the Financial Integrity Network, Juan Zarate, for so generously giving his strategic advice, time, and insights to refine our analysis and recommendations. We are also grateful to Jeff Ross for his insights. This project would not have been possible without the dedicated work of Roksana Gabidullina, who oversaw the organization and execution of this research effort. Finally, we are thankful for the entire Europe, Russia, and Eurasia Program team and their support.

This report is part one of a larger research effort to produce specific recommendations for U.S. policymakers to best tackle great power competition.

This product was funded by the U.S. Department of Homeland Security (DHS), but any opinions expressed by the authors are independent of any funding or sponsorship. Any opinions, arguments, viewpoints, conclusions, or recommendations expressed by the authors herein do not represent those of DHS or the U.S. government.

The research and writing of this report was completed in 2021.

Contents

Executive Summary

Understanding Strategic Competition and Economic Warfare in the Twenty-First Century

Over the past 10 years, the U.S. government has slowly reoriented its foreign and security policy from the fight against global terrorism toward strategic competition with Russia and China. This reorientation has been accompanied by a new examination of how strategic competition will impact the integrity and future stability of the U.S. economy and financial system.

One of the most important elements of strategic competition is sub-threshold warfare (also called asymmetric, hybrid, or gray zone warfare). This emphasis on sub-threshold activities suggests that the adversary does not wish to openly confront the United States but instead seeks to weaken it from within and separate it from its allies.[1] In other words, strategic competitors seek to shape the geostrategic environment in their favor, from information operations to economic warfare—which includes such tools as illicit finance and strategic corruption.

Strategic competitors present a clear economic and financial threat to the United States when they operate in the emerging **financial gray zone**, in which malign actors can take advantage of the U.S. financial system to further their aims and disarm the country internally. For the past three decades, U.S. policy has aimed to successfully integrate Russia and China in the international financial and trade system. Today, this deep, global integration, compounded by Russia and China's malign cyber capabilities, presents a grave challenge to the United States.

The financial gray zone is broadly comprised of four key elements: (1) endemic corruption, (2) illicit financing and money laundering, (3) acquisition of strategic assets and theft of state secrets, and (4) sanctions evasion and decoupling (including through cryptocurrencies). While China and Russia have adopted different approaches to sub-threshold economic competition and their tactics have and will continue to evolve, both seek the same end: to challenge the U.S.-led global economic and financial

order to reduce the United States' influence globally and within these institutions.

Malign cyber activities deployed by state and non-state actors feature prominently in the financial gray zone, particularly cybercrime. The future of cybercrime is closely tied to the future of Russian, Chinese, Iranian, and North Korean foreign policies, as these actors have used a variety of operations to gain tactical advantage. Cryptocurrencies in particular will be an important element of cyber and economic competition, be it for criminal purposes or centralized currency creation. Indeed, for ransomware, phishing scams, or fraud schemes, cryptocurrencies are a preferred mode of payment for cybercriminals.[2]

In addition, the exploration and advancement of central bank digital currencies (CBDCs),[3] in which China is a leader, creates its own set of challenges for the existing financial system along with many uncertainties. Importantly, the proliferation of CBDCs will have serious geopolitical effects, in particular the creation of alternatives to the U.S. dollar and U.S. leadership of the global financial system. This risks reducing the impact of U.S. sanctions policy and undermining U.S. economic power.[4]

The U.S. government, along with its allies, has only begun to acknowledge the sweeping nature of the financial gray zone and to reposition itself to compete within it. Because adversaries exploit the seams between the internal and external policies and authorities, Washington must have greater insights into a complex operating system and better integrate data across the many relevant agencies—in a way, connecting the financial dots. As it develops this comprehensive picture, the U.S. government should develop stronger defensive and offensive policy tools to counter this emerging threat.

1

The Nature of Strategic Competition in the Twenty-First Century

The 2017 U.S. National Security Strategy reoriented U.S. foreign and security policy away from the fight against global terrorism and its financing—to which it had dedicated itself for the past 16 years—and toward strategic competition with Russia and China. The strategy also aimed to respond to regional malign behavior from Iran and North Korea and noted that "many actors have become skilled at operating below the threshold of military conflict—challenging the United States, our allies, and our partners with hostile actions cloaked in deniability."[5]

The 2021 U.S. Interim National Security Strategic Guidance reinforces this new reality by recognizing the "strategic challenges from an increasingly assertive China and destabilizing Russia."[6] It highlights in particular "corruption, which rots democracy from the inside and is increasingly weaponized by authoritarian states to undermine democratic institutions."[7] This strategic view was ultimately presented in a policy memo establishing anti-corruption efforts as a core U.S. national security interest, crystallizing years of policy evolution in that direction among the U.S. national security establishment.[8]

Strategic rivalry or conflict has always included sub-threshold warfare (also called asymmetric, hybrid, or gray zone warfare), but the lack of economic integration between the United States and the Soviet Union and global economic interdependence during the Cold War reduced U.S. understanding of how its adversaries have now fully embraced sub-threshold economic tactics and weaponized use of the U.S. financial system over the last decade. Why do U.S. adversaries increasingly turn to these tactics? It is in part due to U.S. global military dominance; the costs of action and failure in an open military confrontation with the United States are simply too high. In lieu of open military confrontation, the adversary has instead attempted to shape the new battlespaces in its favor, from information operations to economic warfare. It creates constraints on the United States and its allies' ability to respond to adversarial moves—particularly in regions of interest to the opponent—while shielding

itself from retaliatory policy actions. These hybrid methods also seek to sow division within the United States, Europe, and other partner countries.[9]

For example, Russia has used a mix of overt actions and sub-threshold tactics in neighboring Georgia, Ukraine, and Moldova to impede their sovereignty, just as China has done in the South and East China Seas. The aim is to control and dominate their respective "spheres of influence" while reducing the global costs of such actions. One way to reduce these costs is to co-opt pliant political elites to limit negative policy response following aggressive moves. Another is to use economic and technological leverage to deter or ultimately punish countries that impose sanctions or criticize the actions of the adversary. The last recourse of the adversary is to reduce financial exposure to the U.S. financial system as well as to Western institutions to limit the impact of Western sanctions or, in some instances, escalate military tensions to secure future concessions as the West seeks to avoid military conflict. The adversary thus exploits weaknesses (corruption, limited oversight), gaps in legal frameworks, and blind spots to gain long-term advantages. It is an all-encompassing strategy.

This is the twenty-first-century battlespace the U.S. national security community navigates today and in which it must learn to compete more effectively. Every element of democratic principles, norms, institutions, and societies can be exploited and weaponized: information, the global financial system, culture, religion, migration, and democratic institutions themselves. Of all of these, economic and financial competition has been a particularly contested space. The U.S. government, along with its allies, has only begun to acknowledge the sweeping nature of this challenge, including its internal aspects. It must now eliminate the seams between the internal and external policies and authorities, create greater integrated situational awareness, and develop stronger defensive and offensive policy tools to counter it.

The Nature of Economic Warfare

A clearer picture of the growing economic and financial threat to the United States emanating from strategic competition is coming into focus: in this financial gray zone, malign actors take advantage of the U.S. financial system to further their aims and disarm the country internally. The 2020 National Strategy for Combating Terrorist and Other Illicit Financing confirms this by noting that "the same strengths that make the United States an attractive destination for legitimate investment—a large economy; an open business climate; and the central role U.S. financial institutions and the U.S. dollar play in global trade, investment, and financial services—also can attract criminals and other illicit actors seeking to hide or disguise their ill-gotten gains or fund their dangerous plots."[10] The June 2, 2021, National Security Memorandum on the fight against corruption further highlights authoritarian leaders' use of corruption to "undermine democracies worldwide" and the laundering of illicit wealth in the United States and other democracies.[11]

While China and Russia have adopted different approaches to this economic competition and their tactics have and will continue to evolve, both seek the same end: to challenge the U.S.-led global economic and financial order to reduce the United States' influence globally and within these institutions. One important manifestation of this challenge is the movement to decouple altogether from the U.S.-led financial system to create a separate financial system that meets these countries' authoritarian needs and protects them from Western-imposed economic coercion. As a result, a dangerous nexus of strategic competition, state-sponsored illicit finance, corruption, malign influence, and financial decoupling is emerging, all of which threaten U.S. national security interests.

The United States has placed itself at the center of the fight against state-sponsored illicit finance because it is the central node of the global financial system. An estimated $300 billion in proceeds of domestic financial crime is laundered every year in the United States, not including illicit funds coming in from abroad.[12] Indeed, "'following the money' from overseas corruption cases has often led American experts uncomfortably close to home,"[13] which further underscores the strategic seam that adversaries exploit between internal "enablers" and external adversaries. The centrality of the U.S. role is reinforced by the primacy of the U.S. dollar as the worldwide reserve currency. The 2017 National Security Strategy recognized that "economic tools—including sanctions, anti-money laundering and anti-corruption measures, and enforcement actions—can be important parts of broader strategies to deter, coerce, and constrain adversaries."[14] This confers large powers of interdiction, sanctioning, and coercion to the U.S. government, but also means the dollar is at equal risk from launderers, counterfeiters, and other corrupt individuals seeking to hide funds in U.S. dollars.

The Costs of Illicit Finance & Corruption

$2 TRILLION (EST.) [1]

in annual illicit proceeds from transnational criminal groups, kleptocrats, terrorist groups, drug cartels, traffickers

$1 TRILLION [2]

in annual lost tax revenue worldwide and $2.6 trillion stolen due to corruption

$1 TRILLION [3]

paid in bribes annually

$300 BILLION (EST.) [4]

in annual proceeds of domestic financial crime laundered in the United States

$1.3 BILLION [5]

in losses due to internet-enabled crimes (2016)

1. M. Kendall Day, Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, Testimony before the Senate Committee on Banking, Housing, and Urban Affairs, January 17, 2018, https://www.banking.senate.gov/imo/media/doc/Day%20Testimony%201-17-18.pdf.

2. Rodrigo Campos, "Corruption costs $1 trillion in tax revenue globally: IMF," Reuters, April 4, 2019, https://www.reuters.com/article/us-imf-corruption/corruption-costs-1-trillion-in-tax-revenue-globally-imf-idUSKCN1RG1R2; UN News, "The costs of corruption: values, economic development under assault, trillions lost, says Guterres," December 9, 2018, https://news.un.org/en/story/2018/12/1027971.

3. U.S. Department of the Treasury, "National Money Laundering Risk Assessment," 2018, https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf.

4. Ibid.

5. Ibid.

It is therefore not surprising that one of Russia's most powerful non-military tools is its abuse of the international financial system to fund a range of malign influence operations that weaken the United States and its allies internally while economically sustaining the Kremlin's inner circle.[15] China also leverages the size of its internal market and its financial largesse overseas (directed through its Belt and Road and Digital Silk Road Initiatives) to gain strategic advantage and achieve economic dominance. Beijing has combined this with economic espionage and loan pressure to obtain leverage

particularly over smaller countries, most visibly Montenegro—a NATO member—and Sri Lanka.[16] Both China and Russia champion a form of "competitive authoritarian capitalism" that uses state-owned enterprises as well as private elements to protect and grow state interests in strategic industries, an insidious perversion of free markets.[17]

Surveying the Financial Gray Zone

The National Strategy for Combating Terrorist and Other Illicit Financing underscores how corrupt foreign officials have attempted (and at times succeeded) to move funds through the U.S. financial system in ways that undermine U.S. interests and goals through a variety of means—from the use of proxies to decoupling tactics using cryptocurrencies.[18] Competitors blend legal and illegal means together, both complex and cross-border, to make detection more difficult and to achieve their aims within the financial gray zone.

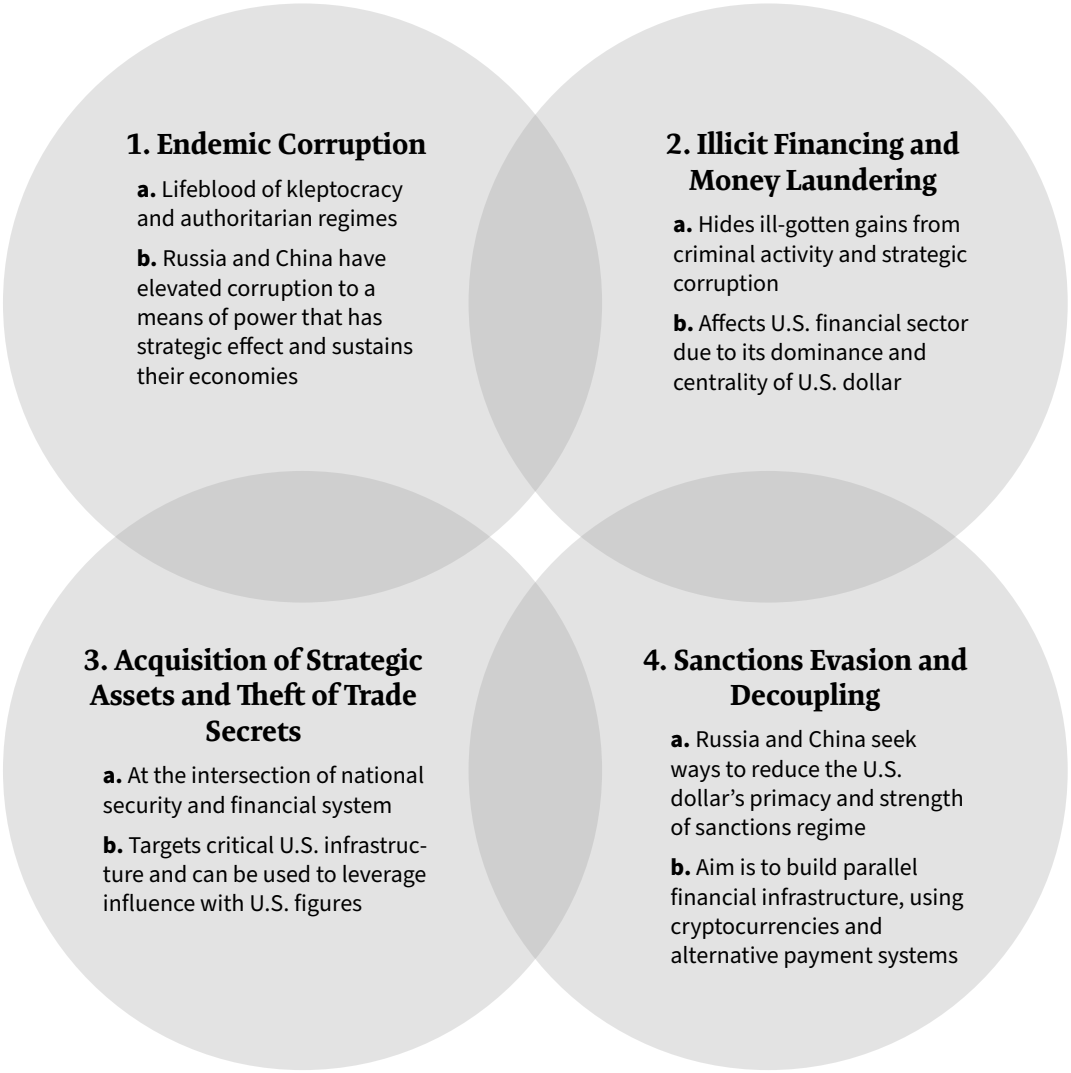
Like sub-threshold warfare, financial crime—including within the U.S. system—is nothing new. Some of the most high-profile criminals perpetrated or were caught on financial charges; Al Capone served his last and longest prison term on a tax evasion conviction.[19] Pablo Escobar laundered a substantial portion of his drug money through professional launderers in Colombia and U.S. bank accounts, allowing U.S. law enforcement to freeze them.[20]

However, in the past 20 years, with globalization and technological advancements, financial crimes have expanded into a form of economic warfare. As the financial system has digitized, it would be difficult today to raid Escobar's money launderers and obtain physical records containing a smoking gun. The financial system has grown more transnational and complex, with webs of anonymous shell companies and transaction schemes obscuring the source of funds through layering processes, not to mention the speed of transactions.[21] This complexity will intensify with the advent of financial technologies (e.g., blockchain) and cryptocurrencies (discussed below), which can both help and hinder transparency.

The list of actors using the system has also expanded beyond criminals to include state officials and regime-affiliated oligarchs. Today, Russia and China present the biggest financial threats because of their size (particularly China), deep global economic and financial integration, and malign cyber capabilities. They can also leverage their position to assist smaller malign actors or connect with transnational organized crime to increase plausible deniability.[22] Indeed, other actors, such as Iran or Venezuela, have sought to evade U.S. sanctions or primacy over the financial systems, using complex financial constructions (e.g., shell companies, proxies) or cryptocurrencies.[23] Transnational crime organizations are still very much a part of these illicit schemes.

With this evolution in mind, the emerging financial gray zone is broadly comprised of four key elements: (1) endemic corruption, (2) illicit financing and money laundering, (3) acquisition of strategic assets and theft of state secrets, and (4) sanctions evasion and decoupling (including through cryptocurrencies). With fraud schemes increasingly enabled by technology, future threats will continue to emanate from cybercrime and these new payment and currency systems.[24]

The Four Elements of the Financial Gray Zone



Source: Authors' research findings.

1. Corruption

Corruption: "The alleged or reported exercise of one's power, position, or resources in order to exploit or exert undue influence over businesses, individuals, or state bodies and institutions, typically through nontransparent and questionable means. This may include actions that could be deliberate and/or unlawful, but may not necessarily be so."[25]

Kleptocracy: "Government by those who seek chiefly status and personal gain at the expense of the governed";[26] "the word means literally, rule by thieves, and describes the specific corruption that occurs when state leaders, generally from poorer countries, routinely loot millions or even billions of dollars from their national treasuries. All too often, the money is spent or stashed in rich countries."[27]

Corruption is the lifeblood of kleptocracy and increasingly of authoritarian regimes; it is the lubricant in the "unvirtuous cycle" of influence, whereby an opaque network of patronage is cultivated and fed, with the ultimate aim to influence decisionmaking to Russia or China's advantage.[28] These regimes have increasingly used "strategic" corruption: bribes and other tools of corruption have become "core instruments of national strategy, leveraged to gain specific policy outcomes and to condition the wider political environment in targeted countries."[29] Through money laundering and other forms of "dirty money," the proceeds of corruption are easily converted into "new domestic and international sources of power and authority."[30]

Corruption has gone from an end in itself (getting rich) to a means (corrupting adversaries from within or securing political power), although it also relies on or connects with other tools such as the ones listed below (sanctions evasion, acquisition of strategic assets). Not only have Russia and China elevated corruption to a tactical instrument of power that has strategic effect, this strategy also sustains these non-democratic regimes' economies.[31] It can also further regimes' quest for internal control through "anti-corruption" drives that target specific actors rather than true corrupt networks in a given country, for example in China, Russia, or Saudi Arabia. This in turn offers a model for other countries to emulate while directly challenging long-standing U.S. anti-corruption or anti-kleptocracy strategies.

It is important to differentiate between authoritarian regimes and their populations, who largely do not support corrupt practices and suffer directly from institutionalized corruption and lower living standards. On the contrary, these regimes increasingly require complex illicit schemes to hide corruption from their citizens, which is why investigative journalists, whistleblowers, anti-corruption political forces, and civil society organizations have come under tremendous pressure—they are a threat to regime survival.

These dynamics matter to the U.S. financial and economic system because a significant portion of these corrupt practices transit through U.S. infrastructure or use the U.S. dollar. Unfortunately, there is also a demand signal for these types of practices in the United States, particularly given the crucial role the U.S. financial system plays in providing access to capital for financial actors across the world. For example, in the infamous 1MDB scandal, U.S. bank Goldman Sachs allegedly helped raise $6.5 billion for the fund from which implicated individuals stole billions (the bank underwrote the bond issues).[32] In this case, a U.S. financial institution provided access to capital markets and financial vehicles that in turn helped leverage more funds. Furthermore, by creating the appearance of policy-for-sale through political funding and hiding the proceeds of foreign corruption in the United States, kleptocratic and authoritarian regimes can degrade the U.S. financial system's integrity as well as the public's trust in it.

Illicit funds that circulate in the U.S. financial system can also be used in malign influence operations against the United States and its allies, in effect corroding democracy from within. In their most extreme form, corruption cases can bring about the compromise or demise of a government once the corruption is exposed, leaving that country in an unstable situation while the outside actors who contributed to it are left undisturbed.[33]

It is for these reasons that the U.S. government has increasingly resorted to sanctioning serious corruption by senior government and former government officials in allied nations, such as Bulgaria and Albania.[34] The new administration has also targeted the kind of corruption that is related to or fosters regional instability, such as in the Western Balkans. A recent executive order targets, among other things, "widespread corruption within various governments and institutions in the Western

Balkans, [which] stymies progress toward effective and democratic governance and full integration into transatlantic institutions, and thereby constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States."[35]

2. Illicit Finance

Strategic corruption finds ways to hide ill-gotten gains and to deploy some of them against the United States and its allies, for example to fund election interference.[36] While attempting to launder illegitimate cash through purchases of real estate and luxury services is nothing new, adversaries show an increasingly sophisticated use of such financing tools as money laundering or letterbox companies. These tools combined have an outsized effect on regional or even national economies.

Although these schemes in isolation may fall below the threshold of illegality, in their totality, they create a complex illicit web that interacts with or penetrates the U.S. financial sector repeatedly.[37] The complex system of anonymous companies and pass-throughs has also created a problematic demand side: some U.S. states have benefited from limited—if not inexistent—regulation of these companies, through fees and tax revenue (e.g., Delaware, Nevada).[38] These states would argue the sector is well regulated, but the issue really lies with the fact that the legal system and the race to attract more companies facilitates the obfuscation of ultimate beneficial ownership (UBO) and the actor who is directing the actions of a given company. Additional beneficiaries are the U.S. dollar and financial system themselves, which have become "magnets for illicit money from around the world." This ability to move money abroad through the U.S. system also helps create an unvirtuous cycle of influence whereby economic and political networks feed off of each other.[39]

Some of the locations and corporate service providers facilitating the flow of illicit money have become unwitting (and sometimes witting) financial gray zone enablers, allowing bad actors to achieve their end and avoid the consequences of the initial act that requires funds to be laundered or moved. One of the most prominent channels to do so is through corporate service providers, which are "any company or sole practitioner whose business is to: form companies or other legal persons; provide a registered office, business address . . . for a company . . . ; act or arrange for another person to act as a: director or secretary of a company . . . trustee of an express trust . . . [or] nominee shareholder for another person."[40]

These "facilitators" play a role in furthering illicit schemes for both malign state actors and transnational organized crime groups.[41] They contribute to the size of foreign direct investment (FDI) flows into certain countries and states (including in real estate and strategic sectors like energy) and their onward movement to offshore financial centers. They also make it increasingly difficult to disentangle the huge inflows of Russian capital from other sources by layering and obfuscating the source of these funds. These facilitators tend to have looser due diligence or enforcement standards, which increases the attraction for their use by malign actors and incentivizes these actors to maintain the conditions that allow for their practices. These services may not be outright illegal (e.g., tax avoidance rather than evasion) but they can blur the line of legality, for example by shifting some companies' tax burden around through complex company structures that also hide the ultimate beneficial owner.

Banks are also exposed to abuse and undue influence, particularly in countries with deep economic ties to Russia or China—or correspondent accounts for those banks. At times, an increase in compliance efforts may trigger a loss of revenue by jeopardizing financial flows from these countries.

Illicit Finance and National Security

The Case of ABLV

PROFILE

- Largest non-resident deposits bank in Latvia; financial bridge between former Soviet states and European and U.S. financial systems
- 90 percent of customers are high risk (per ABLV's risk rating), mostly shell companies registered outside Latvia and in secrecy jurisdictions

FINDINGS OF U.S. TREASURY

- Institutionalized money laundering as a pillar of ABLV's business practices
- Processed funds from a Russia-based bank in a manner consistent with illicit transfer of assets (asset stripping)
- Assisted customers in circumventing foreign currency controls
- Facilitated public corruption through provision of shell company accounts for corrupt politically exposed persons from former Soviet states

ILLICIT FINANCE AND U.S. NATIONAL SECURITY RISKS

- Transactions processed for shell companies owned or controlled by illicit actors potentially assisted transnational organized crime, corruption, and sanctions evasion
- Bank processed transactions for parties connected to U.S.- and UN-designated entities, including companies linked to North Korea's ballistic-missile program
- Jeopardized integrity of U.S. dollar through indirect correspondent accounts
- Allowed corrupt actors to transfer capital abroad through opaque structures, avoiding scrutiny and furthering corruption and capital flight
- Bank executives used bribery to influence Latvian officials and attempt to prevent enforcement and regulatory requirements

U.S. RESPONSE

- ABLV designated as "foreign bank of primary money laundering concern"
- Prohibition on opening or maintaining correspondent accounts for or on behalf of ABLV in the United States

Source: U.S. Department of the Treasury Financial Crimes Enforcement Network, "Proposal of Special Measure Against ABLV Bank, AS as a Financial Institution of Primary Money Laundering Concern," Federal Register 83, no. 33 (February 16, 2018), https://www.fincen.gov/sites/default/files/federal_register_notices/2018-02-16/2018-03214.pdf.

Both big and small banks are exposed to such risks, and smaller outfits can often fly under the radar of law enforcement, benefiting from a lack of vigorous oversight in some jurisdictions.[42] Although red flags have been raised about such practices, financial institutions and government regulators have been slow to act.

Several financial scandals in recent years—long-running and involving billions of dollars—have revealed this financial gray zone in which corrupt foreign officials, state-owned companies, and transnational organized crime networks use shell companies, tax havens, and corporate service providers, among others, to deploy complex financial schemes. In the most shocking case of money laundering of the past 20 years, the Estonian branch of Danish bank Danske Bank was found in 2018 to have laundered around €200 billion between 2007 and 2015 for entities from Russia and former Soviet states, through many transactions and accounts.[43] Earlier that year, the U.S. Treasury Department accused another Baltic bank (this time in Latvia), ABLV, of "institutionalized money laundering" and enabling transfers that supported North Korea's nuclear program; this led to the closure of the bank entirely.[44] In the case of ABLV, the risk to the United States came in part from correspondent accounts that could be used for laundering and sanctions evasion.[45] (The Latvian banking sector has long struggled with institutional money laundering; as early as 2005, the U.S. Treasury designated Multibanka and VEF Bank as two institutions of primary money-laundering concerns, labeling them "a danger to the international community because they facilitate the placement and movement of dirty money in the global financial system.")[46]

The U.S. Congress has passed or introduced several pieces of legislation to fight this threat of illicit finance in recent years, from the Corporate Transparency Act (requiring more information be provided to the Treasury Department's Financial Crimes Enforcement Network, or FinCEN, upon company formation in the United States, including beneficial ownership) to the Countering Russian and Other Overseas Kleptocracy (CROOK) Act (creating an anti-corruption fund to combat public corruption, kleptocracy, and illicit finance).[47]

3. Acquisition of Strategic Assets and Theft of Trade Secrets

The third element of the financial gray zone concerns foreign acquisition of strategic assets and financial technologies ("fintech") and the theft or attempted theft of U.S. trade secrets. Such operations both target critical U.S. infrastructure (new technologies, supply chain safety) and use the U.S. financial infrastructure. As such, this element lies at the intersection of national security and the financial system and at times can be used to leverage influence with U.S. figures. In addition to acquisitions, theft of trade secrets also operates in this nexus of finance and strategic competition, particularly as the demand for technological development and innovation intensifies. The development of these new technologies, the enhanced security measures surrounding them, and resilience of supply chains will be vital to successful competition in the coming decades.

In some cases, the acquisition of technological assets or companies appears benign and is welcome by countries that support open and free trade, or ones that share mutual economic interests with the acquiring country (increasingly China). However, a lack of intelligence resources, an attractive offer, or a seemingly low investment can prevent scrutiny of a takeover that has national security implications. In Denmark, for example, Chinese company Geely Holding Group acquired 51 percent of Saxo Bank in 2017, establishing a technological joint venture that would in turn provide financial and regulatory tech solutions to China's fintech sector and its financial institutions.[48]

Strategic competitors can also focus on the purchase of non-tech strategic assets to influence, circumvent, or alter economic sanctions. A long-running saga over an aluminum mill in Kentucky further exemplifies these dynamics, mixing penetration of a strategic sector, sanctions, and investment into the U.S. economy. In 2018, U.S. company Braidy Industries (now called Unity Aluminum) broke ground on a $1.7 billion aluminum mill in an economically depressed area of northeastern Kentucky. In January 2019, Russian aluminum giant Rusal (owned by the EN+ Group), led by Russian oligarch and Kremlin insider Oleg Deripaska, offered to invest in the project. Rusal, then under sanctions, would invest $200 million in the aluminum mill, giving it a 40 percent ownership stake in the plant.[49] After this initial penetration of a strategic sector, Rusal suggested at the time it would begin to explore more states for future investments in addition to Kentucky.[50]

Although some members of Congress requested a Treasury review of the investment by the Committee on Foreign Investment in the United States (CFIUS), it is unclear if this greenfield investment can be covered by such a review (as opposed to an acquisition).[51] EN+ and Rusal were taken off the sanctions list in January 2019, allowing these investments to flow through the U.S. system once again despite Deripaska's alleged maintained control over some of these assets.[52] So far, Rusal has contributed $75 million to the mill and awaits other funders' decision to complete the $200 million pledge.[53] Difficulty in funding the full project risks giving leverage to Rusal and its 40 percent stake.

4. Sanctions Evasion, Decoupling, and Cryptocurrencies

Finally, strategic competitors use financial tools to evade sanctions and find ways to decouple from the U.S. financial system and the dollar's primacy. Indeed, most cross-border trade is conducted in dollars, conferring huge financial and political leverage onto U.S. financial and law enforcement agencies.

In some cases, certain sanctions evasion efforts have been channeled through the U.S. financial infrastructure; in others, decoupling efforts seek to build a parallel infrastructure that would diminish the U.S. power of economic coercion and financial interdiction. Decoupling could also support attempts to evade sanctions and will be the area to watch in coming years, as financial technology, blockchain technology, and digital currencies present the most forward-looking threats.

> *Digital currency and cryptocurrency*: "A form of currency that is available only in digital or electronic form, and not in physical form. It is also called digital money, electronic money, electronic currency, or cyber cash."[54] Digital currency is "intangible and can only be owned and transacted in by using computers or electronic wallets connected to the Internet or the designated networks."[55] Cryptocurrencies are "a type of digital currency created from software in which a network of independent computer nodes confirms transactions through a decentralized consensus mechanism."[56]
>
> *Central bank digital currency*: "A central bank digital currency (CBDC) uses an electronic record or digital token to represent the virtual form of a fiat currency of a particular nation (or region). A CBDC is centralized; it is issued and regulated by the competent monetary authority of the country."[57]
>
> *Blockchain*: A distributed ledger or digital database "containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network."[58] It "can be public and permissionless, which means any computer node can connect to the network to confirm and validate transactions. There also are private, permissioned blockchains where a central authority or a consortium determines the nodes in

the network. Permissioned blockchains may use aspects of permissionless blockchain software and adapt it to make a private blockchain network."[59]

The search for technological superiority in the financial sector and the desire to lessen the economic impact of future U.S. sanctions have brought Russia and China closer together in their drive to decouple from the international financial system and initiate financial collaboration. In a March 2021 visit to China, Russian foreign minister Sergei Lavrov announced both countries "need to reduce sanctions risks by bolstering [their] technological independence, by switching to payments in [their] national currencies and global currencies that serve as an alternative to the dollar."[60] He added that Russia and China must "move away from using international payment systems controlled by the West."[61] As early as 2017, blockchain companies from both countries began collaborating on blockchain ventures through a joint cryptocurrency fund of $100 million.[62]

Cryptocurrencies and blockchain technology in particular have the potential to build parallel payment and currency systems, from displacing the centrality of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging system to facilitating transactions for sanctioned countries or entities.[63] Specifically, CBDCs, controlled by the state, would pose such a threat (see next section).[64] It is important to note these systems are still years away, and cryptocurrencies from certain states would remain under sanctions in exchanges that fall under U.S. jurisdictions. Nevertheless, the risk exists not only of sanctions evasion through digital currencies but also of sanctions resistance through a diminished U.S. power of financial coercion. A successful, independent system created by China or Russia—or both—could also be exported to other countries and blunt the U.S. financial firepower.

As U.S. policymakers and their allies look ahead, other financial technologies that are harder to control centrally will require scrutiny, for example, social media in-app payments, in-car payments, and other virtual payments that link to a virtual wallet rather than a bank account.

RUSSIA IN THE FINANCIAL GRAY ZONE: THE MASTER CLASS

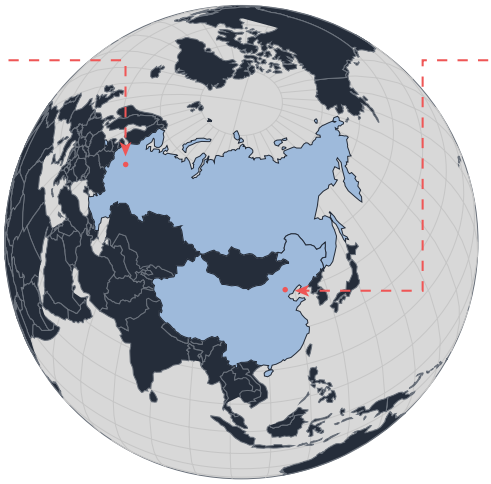
Russia is the primary adversary in the financial gray zone due to its deep connections to the Western economic system and decades of fine-tuning its malign tactics. According to the U.S. Treasury Department, "Russia's integration into the global economic and international financial system presents an especially unique challenge compared to other states subject to U.S. sanctions such as Iran, [or] North Korea. . . . For example, a substantial portion of Russian sovereign bonds are held by external investors, including U.S. pension funds . . . and banks."[65]

Experts have highlighted how, in Russia, the kleptocratic nature of the regime has been exported and corruption transformed into a geopolitical weapon: "The easier it is for Kremlin kleptocrats to launder their money, the easier it is for them to acquire new foot soldiers, new clients, and new corrupt officials in their pay; while abroad they can acquire new lawyers, new lobbyists, and newly compromised politicians to further their agenda."[66]

Russia has also mastered the use of strategic corruption. In places like Eastern Europe and the Baltics, the Kremlin has leveraged corruption to undo democratic and governance progress or enrich regime-affiliated figures.[67] Even closer to home, money allegedly originating from Russian bank accounts and credit cards funded the Kremlin's influence operation in the 2016 U.S. election by, among other things, financially supporting staged protests over divisive issues.[68] The now-infamous Internet Research Agency (IRA) purchased advertisements in the United States through false personas using PayPal and

other means to disparage one candidate and build up divisions.[69] During the 2016, 2018, and 2020 U.S. election cycles, the IRA and other Russian actors allegedly used cryptocurrency accounts to fund additional influence operations, including in Bitcoin to rent servers that would then be used to launch cyber operations to influence the election in 2016.[70]

Adversaries in the Financial Gray Zone



RUSSIA

- Deeply interconnected with Western financial system
- Exports kleptocratic nature of its regime
- Corruption used as a geopolitical weapon to undo democratic progress and finance influence operations
- Repeated use of illicit finance, acquisition of strategic assets and real estate to hide ill-gotten gains or proceeds of corruption

CHINA

- Growing economic weight worldwide and economic ties with U.S. partners
- Corruption as a central piece of flagship Belt and Road Initiative
- Theft of trade secrets and acquisition of strategic assets, particularly in tech sector
- Development of sanctions evasion tools and cryptocurrencies (including central bank digital currency), tightening control of financial digital products

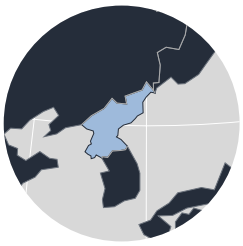
OTHER ACTORS

IRAN

- Use of illicit finance to evade sanctions (e.g., 2012–2014 "gas for gold" scheme with Turkish banks)

NORTH KOREA

- Illicit finance tools to evade sanctions, cybercriminality to fund weapons program



VENEZUELA

- Development of domestic digital currency to avoid sanctions (allegedly with Russian assistance)

Source: Authors' research findings.

One actor in particular has taken this destabilizing behavior worldwide, with full support from the Kremlin. Using his official, front businesses, Yevgeniy Prigozhin, a businessman close to Vladimir Putin, reportedly funds the mercenary private military company Wagner Group.[71] These fronts, some of which were sanctioned by the United States in 2020, operate both in Russia (intimidating journalists and producing fake news) and across the world (running military operations and election

interference). For example, U.S. sanctions focused on Prigozhin's network's abuse of Sudan's natural resources to fund malign activities worldwide and on his use of entities in Hong Kong and Thailand to evade sanctions.[72] Here again, a complex web of front companies is allegedly used to launder money and fund destabilizing operations, as most clearly exemplified by Wagner's activities in Libya (supporting General Hafter and violating UN Security Council resolutions, introducing more weapons into a volatile situation[73]) and the Central African Republic (fighting with government forces against rebel factions, allegedly committing human rights abuses).[74]

Russia has also mastered the use of strategic corruption. In places like Eastern Europe and the Baltics, the Kremlin has leveraged corruption to undo democratic and governance progress or enrich regime-affiliated figures.

CHINA IN THE FINANCIAL GRAY ZONE: LEARNING AND ADAPTING RUSSIA'S TACTICS

While China is a newer entrant to the financial gray zone, it has become a fast learner of Russia's tools and has developed its own approach to hybrid tactics, particularly corruption and the acquisition of strategic assets.

Corruption is a central piece of China's Belt and Road Initiative (BRI), an opaque web of projects with little transparency that creates potential points of leverage for the Chinese regime. In Chad and Uganda, a former CEFC China Energy executive (the company is now state owned) reportedly provided large bribes to grant access to the oil and gas markets to Chinese companies.[75] At the same time, amid a domestic public crackdown on corruption, officials have parked embezzled funds abroad (including in the United States) to hide their schemes and maintain power at home.[76]

In 2019, Chinese telecommunication company Huawei was indicted for theft of trade secrets, perpetrated against U.S. telecoms firm T-Mobile. The attempt allegedly took place both in China and in the United States, and workers were offered bonuses for any valuable information gleaned from this espionage. The charge included wire fraud, once again penetrating the U.S. financial system in the furtherance of other criminal acts and attempts to gain technological superiority.[77]

In an instance more obviously related to national security, in 2019 a U.S.-based engineer was convicted of attempting to illegally export integrated circuits with missile guidance applications to China after gaining unauthorized access to this information.[78] Not only was this transfer aimed at a company placed on the Commerce Department's entity list (representing national security concerns), the engineer used a U.S. limited liability company to channel the funds received from Chinese entities in the trade.[79]

The newest and likely more serious threat in the coming years will be China's development of sanctions evasion tools and decoupling through cryptocurrencies. In the context of another Huawei indictment in 2019, then commerce secretary Wilbur Ross stated that "for years, Chinese firms have broken our export laws and undermined sanctions, often using U.S. financial systems to facilitate their illegal activities."[80]

In this instance, bank fraud, money laundering, and wire fraud charges were pressed in relation to a plot to evade Iran-related sanctions, revolving around a Huawei affiliate in Iran. The plot involved deceiving "numerous global financial institutions and the U.S. government regarding Huawei's business activities in Iran" and relied on Huawei's "global banking relationships for banking services that included processing U.S.-dollar transactions through the United States."[81] Such cases also reaffirm the state-affiliated nature of companies like Huawei, despite claims they are separate from the Chinese Communist Party.[82] It should be noted in this case that it is not yet clear from the public record to what extent Huawei was using its banking relationships to systemically evade sanctions (for itself and to Iran's benefit), or just skirting the normal course of controls in the sector to continue its operations.

The newest and likely more serious threat in the coming years will be China's development of sanctions evasion tools and decoupling through cryptocurrencies.

Despite a crackdown in the past two years on peer-to-peer lending platforms and other financial technology companies, China has invested heavily in research and development of blockchain technology to put the state in control of financial digital products.[83] In 2018, it invested over $3 billion in such projects, showcasing the urgency of the technological race.[84] A renminbi CBDC for cross-border payments would create "controllable anonymity" for the government, providing it with better ways to track currency movement and, with a pilot project linking several central banks (China, Hong Kong, Thailand, United Arab Emirates), would link up multiple CBDC systems under this one currency. In turn, payments for some commodities could increasingly take place in a currency other than the U.S. dollar (for example, oil payments).[85] These initiatives not only risk thwarting U.S. financial firepower, but also increase China's domestic control and international economic power.

OTHER ACTORS ALSO BENEFIT FROM THE GRAY ZONE

Beyond Russia and China, the financial gray zone's tools can serve other actors' purposes, such as North Korea, Iran, or Venezuela. Some of these actors benefit not only from the example set by Beijing and Moscow, but also from their assistance in certain cases.

In one of the most high-profile cases of sanctions evasion, an Iranian-Turkish gold trader orchestrated a $13 billion "gas-for-gold" scheme between 2012 and 2014 (when Iran was still under strict sanctions) through Turkish banks to pay Iran in gold for its natural gas shipments.[86] This scheme involved bank fraud, money laundering, a conspiracy to evade sanctions, and later a lobbying partner in the United States, as was discovered when the case came to trial. The scheme involved complex invoicing methods that are common in illicit finance schemes.

North Korea and Venezuela have benefited from China and Russia's help in lessening the burden of U.S. and international sanctions. In the former case, China and Russia allegedly welcomed North Korean laborers in spite of UN bans. Beijing allowed Chinese firms to conduct business with UN-sanctioned companies that are tied to North Korea's weapons' program while Moscow may have aided the export of North Korean chemical weapons to Syria.[87] The United States also accused Beijing of helping Pyongyang launder money

obtained through cyber theft.[88] The advent of cryptocurrencies has led Venezuela to attempt to evade sanctions as well: during the launch of the petro, the new digital currency, President Nicolás Maduro called it "kryptonite" against the U.S. government's financial firepower. Russian advisers were reportedly involved in the development of the petro, including some with ties to major Russian banks.[89]

The Future of Cyber Activity in Great Power Conflict

CYBERCRIME

Cyber activities feature prominently in the toolbox of authoritarian regimes and have seen increased use in recent years, particularly cybercrime. The future of cybercrime is closely tied to the future of Russian, Chinese, Iranian, and North Korean foreign policies. Right now, cybercrime serves their interests. If there is no change in the policies or leadership of these countries and as long as the cybercriminals in these countries are largely immune to penalty, cybercrime will likely continue to increase. Other countries, such as Brazil and Vietnam, have growing cybercrime communities that outpace law enforcement capabilities, but the principal threat from the four countries is that they are also the geopolitical opponents of the United States.

Cybercrime is a lucrative activity with continued strong growth. It cost the global economy more than a trillion dollars in 2019, and the rate of increase has accelerated since 2010.[90]

Cybercrime harms public safety, undermines national security, and damages economies. The financial sector is a natural target for cybercriminals, who are attracted to both the presence of funds and the troves of sensitive data financial institutions have access to.[91] Besides the economic profit that they can derive from attacking a bank, one should not overlook the strategic effect the disruption of financial services can have for a society. Their status as globally accepted critical infrastructure highlights their systemic importance.[92] Ransomware, phishing schemes, and cryptocurrencies make it easier to succeed and monetize cybercrime and this, combined with the "sanctuary" offered by strategic competitors (who refuse to prosecute cybercriminals), explains the rapid increase.

Cybercrime is a lucrative activity with continued strong growth. It cost the global economy more than a trillion dollars in 2019, and the rate of increase has accelerated since 2010.

The opportunities for criminal activity are also growing as businesses increasingly rely on digital technologies. Faster adoption of new technologies by cybercriminals in Russia and China, such as artificial intelligence (AI) or synthetically generated images (deepfakes), also explains some of the increase in cybercrime. Technological change favors cybercrime, since advanced criminals are often quicker to adopt new technologies (while still relying on old standbys, like phishing). Cyber law enforcement has improved, but operating from sanctuaries helps cybercriminals escape arrest and prosecution. There are thousands of cybercrimes every year, ranging in cost from a few hundred to

tens of millions of dollars.[93] The United States remains a primary target, both for political reasons (no Russian, Chinese, or Iranian hacker will face jail for attacking a U.S. target) and because of the number of lucrative targets, with Europe a close second.

It is important to note that Chinese and Russian cyber operations have significant differences. The Russian state excels at using cyber techniques for coercive action and for conventional political-military espionage, and it tolerates (if not encourages) well-developed cybercriminal networks whose members often have close ties to the state. For example, Roman Seleznev, a successful hacker, was arrested while on vacation in the Maldives. His father is a member of the Russian Duma (or parliament) with ties to the Kremlin.[94] The Russian government continues to object to his arrest, calling it a "kidnapping."[95]

The Russian government rarely directs the activities of these criminal groups, but there are general rules that apply: (1) no attacks on Russian-language targets; (2) help the state if asked; and (3) perhaps share the proceeds of crime with the state. If these rules are observed, cybercriminal groups do not risk interference from Russian law enforcement. Some of the wealthier cybercriminal groups have ties to the Federal Security Service (FSB) in what some analysts call "a complicated relationship between the Russian-speaking cyber underground and the Russian state."[96] This makes Russia the world's premier cybercrime sanctuary. The top Russian cyber groups remain among the most skilled hackers in the world. A British assessment of a few years ago found the top Russian criminal groups to be more skilled at hacking than most national intelligence agencies.[97]

In contrast to Russia, cybercriminals in China are closely controlled by Chinese security services, who often have a directive relationship. Chinese hackers tell of being invited to "drink tea" with local security officials where they are told: "work for us or go to jail." Given the scope of China's domestic surveillance programs, it is next to impossible for a criminal to operate for any period of time without being detected. If Chinese hackers find software vulnerabilities or develop an exploit, they are expected to provide it to the security services at no cost. In exchange, of course, they are provided protection from prosecution. Some hackers become government contractors, operating under the direct control of Chinese agencies. This is crime in the service of the state. China's focus is on theft of intellectual property, commercially valuable information, and military technology.

Like Russia, Iran uses its hackers as a proxy force when needed but gives them the flexibility to engage in hacking for personal gain (mainly against Arab-language and Israeli targets). Iran has a well-organized capability for cyber operations tied to the Iranian Revolutionary Guard (IRG), the Basij (a civilian paramilitary organization directed by the IRG), and the Ministry of Intelligence and Security (MOIS) that uses proxies and contractors, including students.[98] The Basij manages the Iranian "Cyber Army." Basij leaders claim their Cyber Army has over 100,000 volunteer hackers—certainly an exaggeration—but the Basij have close connections with universities and religious schools it can use to recruit students for a proxy hacker force. These proxy hackers can be involved in ransomware. Most incidents are directed at Middle Eastern targets, but in 2018, the U.S. Justice Department indicted two Iranians for a ransomware attack against Atlanta's city government.[99] The Iranian hackers demanded $55,000 worth of bitcoin in payment, and the city would eventually spend approximately $2.6 million recovering from the attack.[100] Iranian hackers have less freedom than their Russian counterparts, but more than Chinese hackers. Iran's cyber police (FATA) do make arrests for cybercrime, but their focus is on political crimes. FATA also enforces laws against "blasphemy" and risqué photos on social media.

North Korea is the least advanced of the cybercrime states, and it is also the most tightly controlled. All North Korean hackers are employees of government intelligence agencies. Their job is to acquire hard currency for Kim Jong-un's regime. Some operate from facilities located outside of the Democratic People's Republic of Korea (DPRK), although Kim prefers tight controls and keeps most hackers in North Korea. China tolerates rather than supports North Korean hacking efforts. The relative low levels of skill of North Korean hackers make them the "bottom feeders," usually going after targets in developing countries.

Cryptocurrencies and ransomware have become central to cybercrime operations. North Korea and Russia both make extensive use of ransomware, which is easily monetized. China and Iran also use ransomware. The other easily monetized hacking activity is the direct theft of financial assets (as when North Korea attempted to extract $951 million from the Bangladeshi Central Bank) and the theft and resale of intellectual property.[101] A UN report estimates that North Korea made a little over $300 million from ransomware attacks in 2019–2020, a significant portion of its national income.[102] Russian actors are much more sophisticated and dangerous, and made much more money, with estimates for ransomware damages in the tens of billions.[103]

The "traditional" ransomware method holds files hostage until a ransom is paid. The latest trend involves exfiltrating data before encrypting it and threatening to make it public. This "double extortion model" circumvents some solutions to ransomware, such as updated backup files, and is intended to weaken a victim's refusal to pay. Ransomware is, however, a manageable threat. Better cyber hygiene and a coordinated international approach can undermine ransomware groups. The supporting cloud infrastructure used by ransomware groups, often located in third countries, could be a target of disruption.

International agreement to reduce cybercrime is making slow progress. While adherence to the Budapest Convention continues to grow (with 64 countries as signatories), the four opponent countries are not adherents.[104] To undercut the Budapest Convention, Russia has been able to win approval for negotiations on a new, global cybercrime convention in the United Nations, part of a larger Russian effort to reshape rules and governance in cyberspace.[105]

Since there is no penalty for criminal groups operating from sanctuaries or with state support, there is no incentive for them to stop. The very uneven nature of cybersecurity practices in many companies means there will still be ample targets for exploitation. Although leading Western banks—after spending hundreds of millions of dollars on their cyber defense—are less likely to be hacked, the same is not true for smaller financial institutions in developing countries. Phishing continues to have a high rate of success and can circumvent many defenses. Finally, commercial software still has many exploitable vulnerabilities—although a new U.S. executive order on cybersecurity will begin to reduce the scope of vulnerability by requiring any software sold to the federal government to meet certain security standards.[106] Given these factors, in combination with continued state sponsorship, as part of a larger geopolitical conflict, there is no reason to expect the level of cybercrime to decline.

Since there is no penalty for criminal groups operating from sanctuaries or with state support, there is no incentive

for them to stop. The very uneven nature of cybersecurity practices in many companies means there will still be ample targets for exploitation.

DIGITAL CURRENCIES

Cryptocurrencies are both full of potential and a serious challenge. Today, a significant portion of cryptocurrency transactions are in support of criminal activity. CBDCs and perhaps private stablecoins will eventually displace cryptocurrencies for all but criminal uses because they are a better store of value and less subject to speculative fluctuations.

Defining Digital Currencies

Decentralized cryptocurrencies have dominated the narrative around digital currencies. The concept of a virtual coin that is not controlled by central banks or regulators gained traction after Bitcoin was launched in 2009. The value of cryptocurrencies has surged over the last few years, with their total market value standing over $2 trillion at the time of writing, up from $260 billion in 2018.[107] Digital currencies still remain a fraction of global markets for stocks, bonds, and gold. There are now thousands of cryptocurrencies available, with varying levels of value and legitimacy, given that it is relatively simple to set them up, and their appeal has become, at times, comedic (e.g., cryptocurrencies named after dogs or issued by hamburger chains). The craze for cryptocurrency has led one token to reach a market value of around $45 billion a day after its launch, a value unrelated to any tangible assets and indicative of the speculative nature of the asset.[108]

Ukraine, Russia, Venezuela, and China are at the top of a 2020 report on global adoption of cryptocurrencies as a common "means of value transfer."[109] Contrary to expectations, cryptocurrencies' primary use is not as a medium of exchange: in one survey, 70 percent of the respondents of a spending survey admitted to using cryptocurrencies to buy more cryptocurrencies.[110] While the use of cryptocurrencies as a medium of exchange for other products and services is not widespread, other surveys also support the conclusion that the more people become users of cryptocurrencies, the more these digital currencies will be used for purchases, rather than exclusively as speculative investments.[111] Their current soaring prices could also drive their use. Cryptocurrencies, as a form of digital currency, are also popular for remittances, thanks to the lower fees they are subject to and because they are simpler and faster to use across borders.

The Risks of Decentralized Digital Currencies

For ransomware, phishing scams, or fraud schemes, cryptocurrencies are a preferred mode of payment for cybercriminals.[112] Cryptocurrency theft amounted to over $520 million in 2020, mainly through hacking of exchanges and decentralized finance (DeFi) platforms.[113] Bitcoin and Ethereum blockchains are also susceptible to "51% attacks," in which criminals control a majority of the decentralized blockchain.[114] Cryptocurrency theft is a major trend in cybercrime, with over $4 billion in cryptocurrency stolen in 2019 and $1.4 billion stolen in the first five months of 2020.[115] These thefts use a combination of tactics including phishing and malware. Cryptojacking is another criminal trend, where malware is installed on victims' computers to remotely mine for cryptocurrencies.[116]

One of the main concerns when it comes to the misuse of cryptocurrencies is their potential for money laundering. While some organizations can provide specific cryptocurrency laundering services, inadequate controls and implementation of anti-money laundering (AML) protocols allow for licit exchanges to liquidate criminals' cryptocurrency.[117] The changing regulatory environment for digital currencies also contributes to the risk and gaps in implementation of the protocols worldwide.[118]

It is not surprising that the surge of decentralized currencies that are not subject to direct control by regulators tempts criminals. The anonymous nature of cryptocurrencies is a further complication for law enforcement's efforts to link transactions to individuals.[119] Ancillary services like coin mixers (a technique used to "launder" cryptocurrencies and hide an account holder's identity) or peer-to-peer exchange platforms provide routes to sidestep attempts from regulators to implement AML controls. However, other support services such as exchanges or wallet providers provide ways to track transactions.[120] Law enforcement agencies, regulators, and policymakers can use these service providers in order to increase compliance and enhance control over activities involving currency exchanges or trading on their sites.

When it comes to converting digital currencies into cash, exchanges, peer-to-peer platforms, and Bitcoin ATMs are the most common choices. While exchanges are subject to know your customer (KYC) and AML controls, lax enforcement contributes to their misuse for illicit activity. Peer-to-peer exchanges allow users to exchange cryptocurrencies for cash in a more decentralized fashion; this direct interaction facilitates money-laundering activities by avoiding the controls more formal exchanges have in place.[121] Bitcoin ATMs can be found around the world, but they are mostly concentrated in the United States.[122] They provide another avenue for anonymity, since most do not require identity verification.[123]

Russians have been attracted to cryptocurrencies since they first appeared. Russian cybercriminals began using cryptocurrencies for cross-border credit card fraud a decade ago. Russians have created numerous cryptocurrency variants, even including Burger King in Russia, which issued "Whoppercoins" that can be redeemed for burgers but also traded on cryptocurrency platforms. However, in 2020 a Russian law made it illegal to purchase goods with cryptocurrencies and categorized decentralized cryptocurrencies as property, triggering reporting requirements for tax purposes.[124]

Cryptocurrencies have been increasingly used to facilitate cybercrime, and scams, darknet markets, theft of funds, and ransomware are the leading crimes for illicit cryptocurrency activity.[125] Some business email compromises request gift cards they can later convert to cryptocurrency.[126] However, the perception that they are uniquely used for that purpose does not hold true. In 2020, under 0.5 percent of Bitcoin's transactions were found to be explicitly illicit.[127] While the illicit share of cryptocurrency activity decreased from 2.1 percent in 2019 to 0.34 percent last year, this is more a reflection of the increased value driven by speculation, which "nearly tripled between 2019 and 2020," rather than a decrease in criminal use.[128]

Stablecoins and Central Bank Digital Currencies

In contrast to these cryptocurrencies, "stablecoins" tie the currency to an asset, rendering them less volatile.[129] One of the most discussed examples of stablecoins came from Facebook's Diem (formerly Libra), announced in 2019. While the Facebook project originally envisioned the offering of multi-currency coin and several single-currency coins—the latter "fully backed by the Reserve, which will

consist of cash or cash equivalents and very short-term government securities denominated in that currency"—it is now anticipated that the initial launch will rely on the U.S. dollar.[130] Tether is another stablecoin backed by reserves and linked to the U.S. dollar.[131] But tying the digital coin to cash is not the only way in which tokens can achieve stability; some are backed by assets such as gold, or even other cryptocurrencies.

The rise of digital payment systems and the popularity of cryptocurrencies and private digital tokens paint a picture of decentralized finance. But multiple countries are currently exploring CBDCs, which represent "a direct claim on a central bank rather than a liability of a private financial institution."[132] They are issued by central banks and are subject to regulation by a country's monetary authority. And while they may sound similar, there are several reasons why a CBDC is different from private digital currencies. CBDCs create their own set of challenges for the existing financial system by threatening to fundamentally change the cost structure of banking and the relationship between central banks, financial institutions, and customers.

The number of countries exploring the potentials of CBDCs continues to grow. According to a BIS survey, 86 percent of all central banks are working on it.[133] Most of them are in exploratory phases, and there are very limited examples of live CBDCs.[134] The Bahamas launched their "Sand Dollar" in October 2020, hoping to increase the efficiency of their payment systems, improve financial inclusion, and reduce money laundering and other illicit cash uses.[135] And while the next few years might see a flurry of activity, most central banks remain in a conceptual research or experimentation phase, and almost two-thirds say they are unlikely to issue a CBDC in the next 24 months.

Most central banks remain in research or pilot phases, and many have so far only issued reports on the feasibility, potential, and challenges of CBDCs. For example, the European Central Bank (ECB) launched a 24-month-long investigation into the digital euro project in July 2021 and expects to begin working on a prototype at the end of 2023.[136] China is one of the most forward-leaning nations when it comes to the launch of its CBDC, the digital yuan, having recently released a white paper detailing the scope of its ambitions.[137] And the U.S. Federal Reserve plans to publish a discussion paper that will explore the possibility of issuing a U.S. CBDC.[138]

The adoption of digital currencies makes sense when considered as part of the "cashless future." They offer lower transaction costs, stability, and speed and ease of payments when compared to current methods.[139] CBDCs, by making anonymity more difficult, could also make the task of law enforcement easier if it develops tools and techniques to take advantage of the data generated by digital transactions, to be able to identify both assets and actors.

"Retail" CBDC would be provided directly to consumers and allow the currency to be used as a form of digital cash. "Wholesale" CBDC would be provided to financial institutions, making it easier to incorporate into existing systems (but possibly more expensive for consumers). Emerging economies have shown special interest in retail CBDC projects, which could expand access to finance services. Wholesale currency could provide benefits to cross-border payments and securities trading.

CBDCs can also play a role in combating money laundering. The ease of tracking CBDC is a clear advantage for this use, especially when compared to cryptocurrencies, as it allows for more transparency and visibility into transaction histories. The need to register and identify in order to access payment methods can improve the tracking of criminal activity while also reducing money laundering.[140]

However, CBDCs raise privacy concerns in contrast to private cryptocurrencies, and this could limit their use.[141] Cybercriminals have proven adept at quickly adopting new technologies and learning how to use them to their advantage. This means that even with the adoption of CBDCs, new and more complicated money-laundering schemes are likely to emerge.[142] As with other digital currencies, licit exchanges can unwittingly facilitate the laundering of virtual tokens. Gaps in regulatory implementation and the identification and exploitation of lax jurisdictions can become a problem for CBDC misuse.[143]

The financial sector has always been a tempting target for cybercriminals. Any infrastructure will present vulnerabilities that cybercriminals can exploit.[144] The introduction of new infrastructures, with untested vulnerabilities such as CBDCs, will also present a new type of direct target for cybercriminals, particularly an increased risk of the potential for data breaches.

Financial and Strategic Implications of CBDCs

The proliferation of CBDCs will have ripple effects on the financial system but should also be understood to have geopolitical effects. Apart from the benefits related to financial inclusion and stability, the issuing of CBDCs can be perceived as a matter of geopolitical strategy. For instance, the EU report on a digital euro considers that the virtual coin may be crucial if, for example, "foreign digital money were to largely displace existing means of payment."[145] Alternatives to the dollar can reduce the impact of sanctions and, some believe, undermine U.S. economic power.[146] The development of CBDCs and the integration of international payment systems could also provide an avenue for countries to avoid dependence on the SWIFT system.[147] Efforts at developing digital currencies by countries like Iran, Russia, and Venezuela demonstrate how some authoritarian governments are beginning to view the future of the global financial infrastructure.[148] These initiatives by themselves will not undermine the current financial ecosystem, but as they evolve coordinately and gain acceptance, they can lead to the creation of an alternate system that skirts control mechanisms currently in place.

Although most central banks used to regard the use of these currencies as trivial, their growing use has led to a change in attitude as they are more widely adopted.[149] If cryptocurrencies or stablecoins become more commonly used for domestic transactions or cross-border payments, the International Monetary Fund's deputy managing director believes a CBDC can be useful as a way of countering "risks to financial stability and [for] monetary policy transmission."[150]

The proliferation of CBDCs will have ripple effects on the financial system but should also be understood to have geopolitical effects. Apart from the benefits related to financial inclusion and stability, the issuing of CBDCs can be perceived as a matter of geopolitical strategy.

Ultimately, there is a paradigm contradiction when it comes to governmental approaches to different forms of digital currencies. While the technology that underpins cryptocurrencies, stablecoins,

and CBDCs can be lumped in the same category, they present wildly different models. Core to cryptocurrencies, like Bitcoin, is an open architecture, relying on decentralization of payments, and peer-to-peer transactionality. The emergence of these virtual currencies is perceived as a threat by some countries, challenging their "ability to maintain control and stability over their country's financial sector."[151] CBDCs are a way in which governments can take advantage of the underlying technology of digital currencies, while maintaining control over payment channels. China, for example, has imposed restrictive measures on private cryptocurrencies and has been testing its digital yuan since April 2020, processing over $300 million in several cities, making it one of the most advanced CBDC projects as earlier noted.[152] In its search for technological leadership, digital currency appears connected to China's developments in robotics, AI, and big data, and to its efforts to displace the dollar as a reserve currency.

Centralizing payments and control over the architecture are antithetical to the paradigm that cryptocurrencies originally introduced. Yet others are embracing the decentralization: in 2021, El Salvador became the first country to adopt Bitcoin as legal tender.[153] Its explicit acceptance of a decentralized model poses a range of questions about governance and processes, and there is skepticism over how successful this experience will ultimately be.[154]

Most CBDCs remain in a research phase, and each design choice and use will carry with it different types of risk or potential criminal uses. How different central banks decide to implement their virtual currency will require addressing different concerns.

Gray Zone Red Flags

Corruption and Illicit Finance

- Accounts or entities under investigation are linked to sanctioned individuals or their families or associates, individuals considered politically exposed persons (PEPs), or individuals with convictions of fraud or money laundering in other jurisdictions.
- Funds under scrutiny (or involved in predicate offense) originate from a high-risk or bank secrecy jurisdiction, a location with permissive or opaque business and legal environment, or a financial institution (FI) with a history of poor practices.
- Transactions or individuals involve or are connected to critical sectors (energy, infrastructure, financial, media) and/or high investment value targets.
- Entities do not perform realistic or logical business activities, or provide incomplete customer due diligence (CDD)/KYC or UBO information in filings (also applies to virtual assets), or constitute a string of shell companies without productive activity tied to each other across multiple high-risk jurisdictions.
- Company, entity, or account is tied to real estate purchases in sensitive or high-value locations (including geographic targeting order [GTO]-covered counties), and/or to accounts flagged by suspicious activity reports (SARs).
- Law firms or lobbyists (potentially with Foreign Agents Registration Act [FARA] filings) are involved in financial activity and company creation (particularly LLCs) for the purpose of real estate purchases or other transactions.

- Transactions in a case or tied to sensitive individuals are made in small amounts, under SAR thresholds, in short period of time; amounts are retrieved shortly thereafter and moved to other accounts in staggered pattern.
- High-value transactions are transferred to accounts then followed by prolonged inactivity (applies to both traditional banking and virtual assets).
- Activity emanates from jurisdictions with highly developed corporate service provider sector and/or strong economic ties with Russia or China, or large national economic players have networks overlapping with Russian and Chinese businesses.

Virtual Assets

- Virtual assets (VAs) are transferred to multiple VA service providers (VASPs) in high-risk jurisdictions and/or jurisdictions with no AML/CFT regulation for VAs.
- VAs are transferred from VASPs to private wallets in short succession in different jurisdictions.
- Transfers are tied to individuals with the same residential or IP addresses, and/or IPs registered in high-risk jurisdiction.
- Transactions involve varied types of VAs, particularly anonymity-enhanced cryptocurrencies.
- Transfers are made first across multiple FIs then to multiple VASPs in short order and/or through registered entities.

For sources referenced in creating this list, please see the endnote section.

About the Authors

Heather A. Conley is former senior vice president for Europe, Eurasia, and the Arctic and director of the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies (CSIS). Prior to joining CSIS as a senior fellow and director for Europe in 2009, Conley served four years as executive director of the Office of the Chairman of the Board at the American National Red Cross. From 2001 to 2005, she was deputy assistant secretary of state in the Bureau of European and Eurasian Affairs with responsibilities for U.S. bilateral relations with the countries of Northern and Central Europe. From 1994 to 2001, she was a senior associate with an international consulting firm led by former U.S. deputy secretary of state Richard L. Armitage. Ms. Conley began her career in the Bureau of Political-Military Affairs at the U.S. Department of State. She was selected to serve as special assistant to the coordinator of U.S. assistance to the newly independent states of the former Soviet Union, and she has received two State Department Meritorious Honor Awards. Ms. Conley is frequently featured as a foreign policy analyst and Europe expert on CNN, MSNBC, BBC, NPR, and PBS, among other prominent media outlets. She received her BA in international studies from West Virginia Wesleyan College and her MA in international relations from the Johns Hopkins University School of Advanced International Studies (SAIS).

James A. Lewis is senior vice president and director of the Strategic Technologies Program at the CSIS. Before joining CSIS, he was a diplomat and a member of the Senior Executive Service. At the Department of State, he worked on a range of political-military issues and was a political adviser to two military commands. Lewis negotiated bilateral agreements on transfers of military technology and regional stability, developed groundbreaking policies on remote sensing and encryption, and led the U.S. delegation to the Wassenaar Arrangement Experts Group. Lewis was the rapporteur for three UN Group of Governmental Experts on Information Security. He leads a long-running track 2 dialogue with the China Institutes of Contemporary International Relations. He has authored numerous publications since coming to CSIS, is frequently quoted in the media, and has testified numerous times before Congress. Lewis is a distinguished visiting professor at the United States Naval Academy's Center for Cyber Security Studies. He received his PhD from the University of Chicago.

Eugenia Lostri is an associate fellow with the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS). Prior to joining CSIS, she was a Tufts University cybersecurity policy fellow at Lawfare and later interned at the Organization of American States. She previously worked as an adviser at the Secretariat for Strategic Affairs in Argentina. Eugenia holds a law degree from the Universidad Católica Argentina and a Master of Laws in International Law from the Fletcher School of Law and Diplomacy.

Donatienne Ruy is the director of the Abshire-Inamori Leadership Academy at CSIS, where she oversees the strategic direction of the program as well as the Executive Education course offering and the Center's internal professional development and training portfolio. She previously worked as an associate fellow with the CSIS Europe, Russia, and Eurasia Program, where she oversaw the program's research portfolios on political developments in the European Union (including EU policy and Brexit), Russian influence in Europe, and Southern Europe and Mediterranean issues.

She supported the program's grant-writing and fundraising efforts for those portfolios and managed the program's European Election Watch platform. She has coauthored such reports as *The Kremlin Playbook 2*, *Restoring the Eastern Mediterranean as a U.S. Strategic Anchor,* and *Crossing Borders: How the Migration Crisis Transformed Europe's External Policy*. Ms. Ruy previously worked at the World Bank on disaster risk financing and insurance, drafting situation reports on natural disaster preparedness in francophone African countries. She received her BA in political science from the Université Libre de Bruxelles in Belgium and her MA in global affairs from the Jackson Institute for Global Affairs at Yale University.

Endnotes

1 U.S. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol. 5: Counterintelligence Threats and Vulnerabilities* (Washington, DC: SSCI, 116th Congress), https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.

2 Palo Alto Networks, *2021 Unit 42 Ransomware Threat Report* (Palo Alto Networks, April 2021), https://www.paloaltonetworks.com/resources/research/unit42-ransomware-threat-report-2021.

3 Committee on Payments and Market Infrastructures, World Bank Group, *Payment aspects of financial inclusion in the fintech era* (Basel: Bank for International Settlements, 2020), 18, https://www.bis.org/cpmi/publ/d191.pdf.

4 Aditi Kumar and Eric Rosenbach, "Could China's Digital Currency Unseat the Dollar?," *Foreign Affairs*, May 20, 2020, https://www.foreignaffairs.com/articles/china/2020-05-20/could-chinas-digital-currency-unseat-dollar.

5 The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 3, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

6 The White House, *Interim National Security Strategic Guidance* (Washington, DC: The White House, March 2021), 14, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

7 Ibid., 19.

8 The White House, "Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest," June 3, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/.

9 U.S. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016*

U.S. Election, Vol. 5: Counterintelligence Threats and Vulnerabilities (Washington, DC: SSCI, 116th Congress), https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.

10 U.S. Department of the Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing* (Washington DC: U.S. Department of the Treasury, February 6, 2020), 7, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf.

11 The White House, "Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest."

12 U.S. Department of the Treasury, *National Money Laundering Risk Assessment* (Washington DC: U.S. Department of the Treasury, 2018), 2, https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf.

13 Nate Sibley and Ben Judah, *Countering Global Kleptocracy: A New US Strategy for Fighting Authoritarian Corruption* (Washington, DC: Hudson Institute, January 2021), 9, https://www.hudson.org/research/16608-countering-global-kleptocracy-a-new-us-strategy-for-fighting-authoritarian-corruption.

14 The White House, *National Security Strategy*, 34.

15 Josh Rudolph and Thomas Morley, *Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies* (Washington DC: The German Marshall Fund of the United States, August 18, 2020), https://securingdemocracy.gmfus.org/covert-foreign-money; see also Heather A. Conley et al., "Countering Russian & Chinese Influence Activities," CSIS, July 2020, https://www.csis.org/features/countering-russian-chinese-influence-activities.

16 While this has at times been dubbed "debt-trap diplomacy," experts have increasingly disputed this term and warned it may be overstated. See for example: Lee Jones and Shahar Hameiri, *Debunking the Myth of 'Debt-trap Diplomacy': How Recipient Countries Shape China's Belt and Road Initiative* (London: Chatham House, August 2020), https://www.chathamhouse.org/2020/08/debunking-myth-debt-trap-diplomacy; to understand the case of the Hambantota Port in Sri Lanka, see Umesh Moramudali, "The Hambantota Port Deal: Myths and Realities," *The Diplomat*, January 1, 2020, https://thediplomat.com/2020/01/the-hambantota-port-deal-myths-and-realities; see also Valerie Hopkins, "Montenegro calls for EU help over $1bn Chinese highway loan," *Financial Times*, April 11, 2021, https://www.ft.com/content/3dd7a516-5352-4f48-bfac-236e43b2342d.

17 Trevor Sutton and Ben Judah, *Turning the Tide on Dirty Money* (Washington, DC: Center for American Progress, February 2021), 11, https://www.americanprogress.org/issues/security/reports/2021/02/26/495402/turning-tide-dirty-money/.

18 U.S. Department of the Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, 21.

19 "Al Capone," Federal Bureau of Investigation, https://www.fbi.gov/history/famous-cases/al-capone.

20 Emily Primeaux, "Murder, money laundering and the demise of Pablo Escobar," Association of Certified Fraud Examiners, September/October 2020, https://www.acfe.com/article.aspx?id=4295011071.

21 Ben Judah and Belinda Li, *Money Laundering for 21st Century Authoritarianism: Western Enablement of Kleptocracy* (Washington, DC: Hudson Institute, December 2017), 19, https://www.hudson.org/research/14020-money-laundering-for-21st-century-authoritarianism.

22 Simon Shuster, "Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions," *Time*, March 20, 2018, https://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency; David Brunnstrom, "U.S. accuses China of 'flagrant' N. Korea violation, offers $5 million reward," Reuters, December 1, 2020, https://www.reuters.com/article/usa-northkorea-china/u-s-accuses-china-of-flagrant-n-korea-violations-offers-5-million-reward-idUSKBN28B540.

23 Jonathan Schanzer, "The Biggest Sanctions-Evasion Scheme in Recent History," *The Atlantic*, January 4, 2018,

https://www.theatlantic.com/international/archive/2018/01/iran-turkey-gold-sanctions-nuclear-zarrab-atilla/549665.

24 U.S. Department of the Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, 9.

25 Heather Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Lanham: CSIS/Rowman & Littlefield, October 13, 2016), https://www.csis.org/analysis/kremlin-playbook.

26 "Kleptocracy," Merriam-Webster.com Dictionary, https://www.merriam-webster.com/dictionary/kleptocracy.

27 Jason Sharman, "On kleptocracy," *Cambridge Alumni Magazine*, Issue 86, March 27, 2019, https://www.cam.ac.uk/kleptocracy.

28 Conley et al., *The Kremlin Playbook*.

29 Philip Zelikow, Eric Edelman, Kristofer Harrison, and Celeste Ward Gventer, "The Rise of Strategic Corruption: How States Weaponize Graft," *Foreign Affairs* 99, no. 4 (July/August 2020), https://www.foreignaffairs.com/articles/united-states/2020-06-09/rise-strategic-corruption.

30 Sutton and Judah, *Turning the Tide*, 10.

31 Josh Rudolph, "Treasury's War on Corruption: A U.S. Treasury Department Strategy to Fight Kleptocracy and Root Dirty Money Out of the U.S. Financial System," German Marshall Fund, December 22, 2020, https://securingdemocracy.gmfus.org/treasurys-war-on-corruption.

32 Rozanna Latiff, "Understanding Goldman Sachs' role in Malaysia's 1MDB mega scandal," Reuters, October 22, 2020, https://www.reuters.com/article/us-goldman-sachs-1mdb-settlement-explain/understanding-goldman-sachs-role-in-malaysias-1mdb-mega-scandal-idUSKBN2772HC.

33 Kit Gillet, "The missing billion," *Politico Europe*, May 14, 2015, https://www.politico.eu/article/moldova-missing-billion.

34 U.S. Department of the Treasury, "Treasury Sanctions Influential Bulgarian Individuals and Their Expansive Networks for Engaging in Corruption," press release, June 2, 2021, https://home.treasury.gov/news/press-releases/jy0208; Llazar Semini, "US sanctions Albania ex-leader Sali Berisha over corruption," ABC News, May 19, 2021, https://abcnews.go.com/International/wireStory/us-sanctions-albania-leader-sali-berisha-corruption-77778773.

35 "Executive Order on Blocking Property and Suspending Entry into the United States of Certain Persons Contributing to the Destabilizing Situation in the Western Balkans," The White House, June 8, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/08/executive-order-on-blocking-property-and-suspending-entry-into-the-united-states-of-certain-persons-contributing-to-the-destabilizing-situation-in-the-western-balkans.

36 Rudolph and Morley, *Covert Foreign Money*.

37 See for example: "The Panama Papers: Exposing the Rogue Offshore Finance Industry," International Consortium of Investigative Journalists, https://www.icij.org/investigations/panama-papers/.

38 Judah and Li, *Money Laundering for 21st Century Authoritarianism*, 20.

39 Heather Conley et al., *The Kremlin Playbook*; "Enhancing National Security by Re-Imagining FinCEN," Global Financial Integrity, March 1, 2021, 1, https://gfintegrity.org/report/enhancing-national-security-by-reimagining-fincen.

40 "Money laundering supervision for trust or company service providers," Government of the United Kingdom, February 25, 2014, https://www.gov.uk/guidance/money-laundering-regulations-trust-or-company-service-

provider-registration.

41 "Transnational Organized Crime: A Growing Threat to National and International Security," Obama administration National Security Council, https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat.

42 Heather Conley et al., *The Kremlin Playbook 2: The Enablers* (Lanham: CSIS/Rowman & Littlefield, March 2019), 24, https://www.csis.org/features/kremlin-playbook-2.

43 Richard Milne and Caroline Binham, "Inside Danske's €200bn 'dirty money' scandal," *Financial Times*, October 3, 2018, https://www.ft.com/content/712f995e-c57b-11e8-bc21-54264d1c4647.

44 Neil Buckley, "Latvia: a banking scandal on the Baltic," *Financial Times*, February 23, 2018, https://www.ft.com/content/e7b586c4-1883-11e8-9376-4a6390addb44.

45 U.S. Department of the Treasury, *Report to Congress Pursuant to Section 243 of the Countering America's Adversaries Through Sanctions Act of 2017 Regarding Interagency Efforts in the United States to Combat Illicit Finance Relating to the Russian Federation* (Washington, DC: U.S. Department of the Treasury, August 2018), 12, https://home.treasury.gov/sites/default/files/2018-08/U_CAATSA_243_Report_FINAL.pdf.

46 U.S. Department of the Treasury, "Treasury Wields PATRIOT Act Powers to Isolate Two Latvian Banks Financial Institutions Identified as Primary Money Laundering Concerns," press release, April 21, 2005, https://www.treasury.gov/press-center/press-releases/Pages/js2401.aspx.

47 U.S. Congress, H.R.2513 – Corporate Transparency Act of 2019, 116th Congress (2019–2020), https://www.congress.gov/bill/116th-congress/house-bill/2513/text?r=2&s=2; U.S. Congress, H.R. 402 – CROOK Act, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/402/text?r=1&s=1.

48 Heather Conley and James A. Lewis, *Chinese Technology Acquisitions in the Nordic Region* (Washington, DC: CSIS, September 24, 2020), 10, https://www.csis.org/analysis/chinese-technology-acquisitions-nordic-region.

49 Kenneth P. Vogel, "Democrats Seek Review of Russian Investment in Kentucky," *New York Times*, May 16, 2019, https://www.nytimes.com/2019/05/16/us/politics/rusal-investment-kentucky.html.

50 "FARA Informational Materials," En+ Group, April 18, 2019, https://efile.fara.gov/docs/6170-Informational-Materials-20190428-63.pdf.

51 Lesley Clark and Kevin G. Hall, "Treasury may review Russian investment in a Kentucky mill," McClatchy, June 4, 2019, https://www.mcclatchydc.com/news/politics-government/congress/article231179818.html.

52 U.S. Department of the Treasury, "OFAC Delists En+, Rusal, and EuroSibEnergo," press release, January 27, 2019, https://home.treasury.gov/news/press-releases/sm592; Kenneth P. Vogel, "Deripaska and Allies Could Benefit From Sanctions Deal, Document Shows," *New York Times*, January 21, 2019, https://www.nytimes.com/2019/01/21/us/politics/oleg-deripaska-russian-sanctions.html?module=inline.

53 Chris Otts, "Aluminum company pleads for more time to build Ky. plant," WDRB, February 18, 2021, https://www.wdrb.com/in-depth/aluminum-company-pleads-for-more-time-to-build-ky-plant/article_bc49816e-722d-11eb-8d1d-237f4faddb3a.html.

54 Jake Frankenfield, "Digital Currency," Investopedia, https://www.investopedia.com/terms/d/digital-currency.asp.

55 Frankenfield, "Digital Currency."

56 Yaya J. Fanusie and Trevor Logan, "Crypto Rogues," Foundation for Defense of Democracies, July 11, 2019, https://www.fdd.org/analysis/2019/07/11/crypto-rogues.

57 "Central Bank Digital Currency (CBDC)," Investopedia, April 6, 2021, https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp.

58 "Blockchain," Merriam-Webster.com Dictionary, https://www.merriam-webster.com/dictionary/blockchain.

59 Fanusie and Logan, "Crypto Rogues."

60 Gabrielle Tétrault-Farber and Andrew Osborn, "Russia's top diplomat starts China visit with call to reduce U.S. dollar use," Reuters, March 22, 2021, https://www.reuters.com/article/us-russia-china-usa-idUSKBN2BE0XH.

61 Tétrault-Farber and Osborn, "Russia's top diplomat."

62 Yaya J. Fanusie, "Seeking Sanctions Resistance Through Blockchain Technology," Foundation for Defense of Democracies, October 11, 2018, https://www.fdd.org/analysis/2018/10/11/seeking-sanctions-resistance-through-blockchain-technology.

63 Yaya J. Fanusie, "Will Crypto Rogues Threaten the Geopolitical Order?" Foundation for Defense of Democracies, July 23, 2019, https://www.fdd.org/analysis/2019/07/23/will-crypto-rogues-threaten-the-geopolitical-order.

64 For more information on the concept and design of CBDCs, see: Stephanie Segal and Pearl Risberg, "Central Bank Digital Currencies, Design Choices, and Impacts on Currency Internationalization" CSIS, *CSIS Briefs*, December 18, 2020, https://www.csis.org/analysis/central-bank-digital-currency-design-choices-and-impacts-currency-internationalization.

65 U.S. Department of the Treasury, *Report to Congress Pursuant to Section 243*, 1.

66 Judah and Li, *Money Laundering for 21st Century Authoritarianism*, 8.

67 Conley et al., *The Kremlin Playbook*.

68 Alliance for Securing Democracy, "Russian government-connected Internet Research Agency utilizes fake social media accounts to mobilize rallies across the United States," German Marshall Fund, https://securingdemocracy.gmfus.org/incident/russian-government-connected-internet-research-agency-utilizes-fake-social-media-accounts-to-mobilize-rallies-across-the-united-states/; see also: Spencer Ackerman, "Mueller Indicts Trump's Claim That Russian Interference Is 'Fake News'," The Daily Beast, February 16, 2018, https://www.thedailybeast.com/mueller-indicts-trumps-claim-that-russian-interference-is-fake-news.

69 IRA Indictments in U.S. District Court for the District of Columbia, Case 1:18-cr-00032-DLF, https://www.justice.gov/file/1035477/download.

70 U.S. Department of the Treasury, "Treasury Sanctions Russia-Linked Election Interference Actors," press release, September 10, 2020, https://home.treasury.gov/news/press-releases/sm1118; Mueller indictment against GRU officers, U.S. District Court for the District of Columbia, Case 1:18-cr-00215-ABJ, filed July 13, 2018, https://www.justice.gov/file/1080281/download.

71 Bellingcat Investigation Team, "Putin Chef's Kisses of Death: Russia's Shadow Army's State-Run Structure Exposed," Bellingcat, August 14, 2020, https://www.bellingcat.com/news/uk-and-europe/2020/08/14/pmc-structure-exposed.

72 U.S. Department of the Treasury, "Treasury Targets Financier's Illicit Sanctions Evasion Activity," press release, July 15, 2020, https://home.treasury.gov/news/press-releases/sm1058.

73 Paul Stronski, "Implausible Deniability: Russia's Private Military Company," Carnegie Endowment for International Peace, June 2, 2020, https://carnegieendowment.org/2020/06/02/implausible-deniability-russia-s-private-military-companies-pub-81954.

74 Luke Harding and Jason Burke, "Russian mercenaries behind human rights abuses in CAR, say UN experts," *The Guardian*, March 30, 2021, https://www.theguardian.com/world/2021/mar/30/russian-mercenaries-accused-of-human-rights-abuses-in-car-un-group-experts-wagner-group-violence-election.

75 Zelikow et al., "The Rise of Strategic Corruption."

76 Frank Shyong, "Ex-wife of fugitive Chinese official will forfeit millions of dollars worth of San Gabriel Valley property in visa fraud case," *Los Angeles Times*, January 11, 2017, http://www.latimes.com/local/lanow/la-me-ln-wife-fugitive-chinese-20170110-story.html; see also: Eli Binder and Katrina Northrop, "China's Global Treasure Map," *The Wire China*, September 20, 2020, https://www.thewirechina.com/2020/09/20/chinas-global-treasure-map/.

77 U.S. Department of Justice, "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice," press release, January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade.

78 U.S. Department of Justice, "Electrical Engineer Convicted of Conspiring to Illegally Export to China Semiconductor Chips with Missile Guidance Applications," press release, July 2, 2019, https://www.justice.gov/opa/pr/electrical-engineer-convicted-conspiring-illegally-export-china-semiconductor-chips-missile.

79 U.S. Department of Justice, "Electrical Engineer Convicted."

80 U.S. Department of Justice, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," press release, January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial.

81 Ibid.

82 Alliance for Securing Democracy, "Chinese telecoms giant Huawei charged in New York with money laundering, bank fraud, wire fraud, conspiracy, and conspiring to obstruct justice," German Marshall Fund, January 28, 2019, https://securingdemocracy.gmfus.org/incident/chinese-telecoms-giant-huawei-charged-in-new-york-with-money-laundering-bank-fraud-wire-fraud-conspiracy-and-conspiring-to-obstruct-justice/.

83 Herbert Poenisch, "China moves towards greater control over fintechs," OMFIF, March 12, 2021, https://www.omfif.org/2021/03/china-moves-towards-greater-control-over-fintechs.

84 Joseph Young, "Can China Pursue Blockchain Innovation Amid Cryptocurrency Ban?," CCN, September 5, 2018, https://www.ccn.com/can-china-pursue-blockchain-innovation-amid-cryptocurrency-ban.

85 Herbert Poenisch, "China is undermining the dollar's global role," OMFIF, April 22, 2021, https://www.omfif.org/2021/04/china-is-undermining-the-dollars-global-role/.

86 Schanzer, "The Biggest Sanctions-Evasion Scheme in Recent History."

87 Samuel Ramani, "Why Russia is openly violating sanctions against North Korea," *Washington Post*, April 23, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/20/why-is-russia-openly-flouting-international-sanctions-against-north-korea/.

88 Brunnstrom, "U.S. accuses China of 'flagrant' N. Korea violation."

89 Shuster, "Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions."

90 James A. Lewis, Zhanna Malekos Smith, Eugenia Lostri, *The Hidden Costs of Cybercrime* (Washington, DC: CSIS, December 9, 2020), https://www.csis.org/analysis/hidden-costs-cybercrime.

91 Cyber Policy Initiative, "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment

for International Peace, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide

92 "Report of the Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security," United Nations, May 28, 2021 https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

93 Lewis, Malekos Smith, and Lostri, *The Hidden Costs of Cybercrime*.

94 Nicole Perlroth, "Russian Hacker Sentenced to 27 Years in Credit Card Case," *New York Times*, April 21, 2017, https://www.nytimes.com/2017/04/21/technology/russian-hacker-sentenced.html

95 Nate Raymond, "Russian lawmaker's son convicted in U.S. for hacking scheme," Reuters, August 25, 2016, https://www.reuters.com/article/us-usa-cyber-creditcards/russian-lawmakers-son-convicted-in-u-s-for-hacking-scheme-idUSKCN1102JJ.

96 Anastasia Sentsova and Yelisey Boguslavskiy, "New Russian Crypto Law - A Government Tool to Take Control Over the DarkWeb Market?," AdvIntel, February 11, 2021, https://www.advanced-intel.com/post/new-russian-crypto-law-a-government-tool-to-take-control-over-the-darkweb-market.

97 Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (London: Chatham House, March 2009), https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0309cyberspace.pdf.

98 Congressional Research Service, *Iranian Offensive Cyber Attack Capabilities* (Washington, DC: Congressional Research Service, January 13, 2020), https://fas.org/sgp/crs/mideast/IF11406.pdf.

99 U.S. Attorney's Office: Northern District of Georgia, "Atlanta U.S. Attorney Charges Iranian nationals for City Of Atlanta ransomware attack," Department of Justice, December 5, 2018, https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack.

100 Lily Hay Newman, "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare," Wired, April 23, 2018, https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

101 Neha Banka, "Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank," The Indian Express, June 30, 2021, https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/

102 Edith Lederer, "UN experts: North Korea using cyber-attacks to update nukes," Associated Press, February 9, 2021, https://apnews.com/article/technology-global-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4a84780f54a3279ef707b33.

103 Associated Press, "How the Kremlin provides a safe harbor for ransomware," NBC News, April 16, 2021, https://www.nbcnews.com/tech/security/kremlin-provides-safe-harbor-ransomware-rcna699.

104 "Convention on Cybercrime," Council of Europe, November 23, 2001, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

105 Allison Peters, "Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime," *Foreign Policy*, September 16, 2019, https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/.

106 "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

107 "Global Cryptocurrency Charts: Total Cryptocurrency Market Cap," CoinMarketCap, https://coinmarketcap.com/charts/.

108 Olga Kharif, "Cryptocurrency's Value Surges to $45 Billion One Day After Its Debut," Bloomberg, May 11, 2021, https://www.bloomberg.com/news/articles/2021-05-11/cryptocurrency-s-value-surges-to-45-billion-after-monday-debut.

109 "The 2020 Global Crypto Adoption Index: Cryptocurrency is a Global Phenomenon," Chainalysis, September 8, 2020, https://blog.chainalysis.com/reports/2020-global-cryptocurrency-adoption-index-2020.

110 "Crypto Spending Report 2020," Blockcard, https://unbanked.com/wp-content/uploads/2021/06/Crypto-Spending-Report-2020.pdf.

111 "2021 Global Crypto User Index", Binance Research, January 28, 2021, https://research.binance.com/en/analysis/global-crypto-user-index-2021.

112 Palo Alto Networks, *2021 Unit 42 Ransomware Threat Report* (Palo Alto Networks, April 2021), https://www.paloaltonetworks.com/resources/research/unit42-ransomware-threat-report-2021.

113 Chainalysis, *The 2021 Crypto Crime Report* (Chainalysis, February 2021), 82, https://go.chainalysis.com/2021-Crypto-Crime-Report.html.

114 Aleksey Studnev, "Attacker Stole 807K ETC in Ethereum Classic 51% Attack," Bitquery, August 5, 2020, https://bitquery.io/blog/attacker-stole-807k-etc-in-ethereum-classic-51-attack.

115 Jeb Suu "Hackers Stole Over $4 Billion From Crypto Crimes In 2019 So Far, Up From $1.7 Billion In All Of 2018," *Forbes*, August 15, 2019, https://www.forbes.com/sites/jeanbaptiste/2019/08/15/hackers-stole-over-4-billion-from-crypto-crimes-in-2019-so-far-up-from-1-7-billion-in-all-of-2018/#1493a0a755f5; Danny Nelson, "Crypto Criminals Have Already Stolen $1.4B in 2020, Says CipherTrace," Coindesk, June 2, 2020, https://www.coindesk.com/crypto-criminals-have-already-stolen-1-4b-in-2020-says-ciphertrace.

116 "Cryptojacking – What is it?" Malwarebytes, https://www.malwarebytes.com/cryptojacking/.

117 Europol, "Multi-million Euro Cryptocurrency Laundering Service Bestmixer.io Taken Down," press release, May 22, 2019, https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down.

118 Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors* (Paris: FATF, July 2018), https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.

119 Nikita Malik, "How Criminals and Terrorists Use Cryptocurrency and How to Stop It," *Forbes*, August 31, 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/?sh=7f35f1cf3990.

120 Billy Bambrough, "Massive Hack Exposes Bitcoins Greatest Weakness," *Forbes*, December 23, 2020, https://www.forbes.com/sites/billybambrough/2020/12/23/massive-hack-exposes-bitcoins-greatest-weakness/?sh=3d8b7104da7d.

121 "Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders," Elliptic, December 9, 2020, https://www.elliptic.co/resources/typologies-concise-guide-crypto-leaders.

122 "Bitcoin ATM and Kiosks," Bitrawr, https://www.bitrawr.com/bitcoin-atms.

123 "Genesis Coin cryptocurrency ATM machine producer," Coin ATM Radar, https://coinatmradar.com/manufacturer/3/genesis-coin-bitcoin-atm-producer/.

124 Anna Baydakova, "Putin Signs Russian Crypto Bill Into Law," CoinDesk, July 31, 2020, https://www.coindesk.

com/putin-signs-russian-crypto-bill-into-law.

125 Tom Wilson, "Just 270 crypto addresses laundered $1.3 billion in dirty funds last year, research shows," Reuters, February 11, 2020, https://www.reuters.com/article/us-crypto-currencies-crime/just-270-crypto-addresses-laundered-1-3-billion-in-dirty-funds-last-year-research-shows-idUSKBN2AB1UD.

126 APWG, *Phishing Activity Trends Report* (Washington DC: APWG, February 9, 2021), https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf.

127 CipherTrace, *Cryptocurrency Crime and Anti-Money Laundering Report* (CipherTrace, February 2021) https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/.

128 Chainalysis, *The 2021 Crypto Crime Report*, 5; Citi GPS: Global Perspectives & Solutions, *Bitcoin at the Tipping Point* (New York: Citi, March 2021), https://ir.citi.com/JTnzeEoMSIAEFlwH12VeM5d%2BCckWNrsO9lxpmy-Wezrz5V%2Bx%2FfRvm0gv6cWRpDHGWtIk7sTME%3D.

129 Lael Brainard, "Digital Currencies, Stablecoins, and the Evolving Payments Landscape," Peterson Institute for International Economics, October 16, 2019, https://www.federalreserve.gov/newsevents/speech/files/brainard20191016a.pdf.

130 "White Paper v2.0: Cover Letter," Libra, https://libra.vin/en-us/white-paper/#cover-letter; Hannah Murphy, "Facebook's Libra currency to launch next year in limited format," *Financial Times*, November 26, 2020, https://www.ft.com/content/cfe4ca11-139a-4d4e-8a65-b3be3a0166be.

131 "Digital money for a digital age," Tether, https://tether.to/.

132 Committee on Payments and Market Infrastructures, World Bank Group, *Payment aspects of financial inclusion in the fintech era* (Basel: Bank for International Settlements, 2020), 18, https://www.bis.org/cpmi/publ/d191.pdf.

133 Codruta Boar and Andreas Wehrli, *Ready, steady, go? – Results of the third BIS survey on central bank digital currency* (Basel: Bank for International Settlements, January 2021), 6, https://www.bis.org/publ/bppdf/bispap114.pdf.

134 PricewaterhouseCoopers, *PwC CBDC global index* (London: PWC, April 2021), https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-cbdc-global-index-1st-edition-april-2021.pdf.

135 "Objectives," Sand Dollar, https://www.sanddollar.bs/objectives.

136 European Central Bank, "Eurosystem launches digital euro project," July 14, 2021, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html; Bjarke Smith-Meyer, "Digital euro bill due early 2023," Politico Europe, February 9, 2022, https://www.politico.eu/article/digital-euro-bill-due-early-2023/.

137 European Central Bank, *Report on a digital euro* (Frankfurt: European Central Bank, October 2020), 19, https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.; "China Release White Paper on CBDC: $5.4B Settled, Smart Contracts Enabled," FinTechs, July 17, 2021, https://fintechs.fi/2021/07/17/china-release-white-paper-on-cbdc-5-4-settled-smart-contracts-enabled/.

138 Nathaniel Popper and Cao Li, "China Charges Ahead With a National Digital Currency," *New York Times*, March 1, 2021, https://www.nytimes.com/2021/03/01/technology/china-national-digital-currency.html; The Federal Reserve, "Federal Reserve Chair Jerome H. Powell outlines the Federal Reserve's response to technological advances driving rapid change in the global payments landscape," press release, May 20, 2021, https://www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm.

139 Boar and Wehrli, *Ready, steady, go?*, 7.

140 Yaya Fanusie, *Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them* (São Paulo: Lawfare, November 2020), https://assets.documentcloud.org/documents/20423765/fanusie-dsc-final-2.pdf.

141 European Central Bank, *Report on a digital euro*; Ibid., 22.

142 Fanusie, "Central Bank Digital Currencies."

143 Ibid.

144 Sarah Allen et al., "Design choices for central bank digital currency," Brookings Institution, July 23, 2020, https://www.brookings.edu/blog/up-front/2020/07/23/design-choices-for-central-bank-digital-currency/.

145 European Central Bank, *Report on a digital euro*.

146 Aditi Kumar and Eric Rosenbach, "Could China's Digital Currency Unseat the Dollar?," Foreign Affairs, May 20, 2020, https://www.foreignaffairs.com/articles/china/2020-05-20/could-chinas-digital-currency-unseat-dollar.

147 Felipe Erazo, "Digital Currencies Could Outshine SWIFT System, Says Central Bank of Russia's Deputy Governor," Bitcoin, December 29, 2020, https://news.bitcoin.com/digital-currencies-could-outshine-swift-system-says-central-bank-of-russias-deputy-governor/.

148 Fanusie, "Will Crypto Rogues Threaten the Geopolitical Order?"

149 Boar and Wehrli, *Ready, steady, go?*, 12.

150 "Deputy Managing Director Tao Zhang's Keynote Address on Central Bank Digital Currency," International Monetary Fund, March 19, 2020, https://www.imf.org/en/News/Articles/2020/03/19/sp031920-deputy-managing-director-tao-zhangs-keynote-address-on-central-bank-digital-currency.

151 Chuyan Cheng, "Digitalize Your Wallet (Cash): China's Digital Currency, Fintech Companies, and Technology Race with the West," CSIS, March 5, 2021, https://www.csis.org/blogs/technology-policy-blog/digitalize-your-wallet-cash-chinas-digital-currency-fintech-companies.

152 "China launches digital currency pilots in four cities," China Perspective, April 20, 2020, https://www.chinaperspective.com/article/FX/china-launches-digital-currency-pilots-in-four-cities.

153 Arjun Kharpal, "El Salvador becomes first country to adopt bitcoin as legal tender after passing law," CNBC, June 8, 2021, https://www.cnbc.com/2021/06/09/el-salvador-proposes-law-to-make-bitcoin-legal-tender.html.

154 See for example: Joanna Ossinger, "El Salvador Move Could Strain Bitcoin Blockchain, JPMorgan Says," Bloomberg, July 11, 2021, https://www.bloomberg.com/news/articles/2021-07-11/jpmorgan-says-el-salvador-move-could-strain-bitcoin-blockchain; Isabelle Lee, "The IMF says it is has legal and economic concerns about El Salvador's move to make bitcoin legal tender," Markets Insider, June 10, 2021, https://markets.businessinsider.com/news/stocks/imf-international-monetary-fund-risk-el-salvador-bitcoin-legal-tender-2021-6?op=1; "World Bank rejects El Salvador request for Bitcoin help," BBC News, June 17, 2021, https://www.bbc.com/news/business-57507386.

Gray Zone Red Flags Sources

Nate Sibley and Ben Judah, *Countering Global Kleptocracy: A New US Strategy for Fighting Authoritarian Corruption* (Washington, DC: Hudson Institute, January 2021), https://www.hudson.org/research/16608-countering-global-leptocracy-a-new-us-strategy-for-fighting-authoritarian-corruption; "High-Risk Jurisdictions subject

to a Call for Action – June 2021," Financial Action Task Force, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-june-2021.html; Ben Judah and Belinda Li, *Money Laundering for 21st Century Authoritarianism* (Washington, DC: Hudson Institute, November 2017), https://www.hudson.org/research/14020-money-laundering-for-21st-century-authoritarianism; Financial Action Task Force, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: Financial Action Task Force, September 2020), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/virtual-assets-red-flag-indicators.html; "Illicit Financial Flows (IFFs)," The World Bank, July 7, 2017, https://www.worldbank.org/en/topic/financialsector/brief/illicit-financial-flows-iffs; OECD, *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors* (Paris: OECD Publishing, 2019), https://www.oecd.org/tax/crime/money-laundering-awareness-handbook.htm; OECD, *Ending the Shell Game: Cracking down on the Professionals who enable Tax and White Collar Crimes* (Paris: OECD Publishing, 2021), https://www.oecd.org/tax/crime/ending-the-shell-game-cracking-down-on-the-professionals-who-enable-tax-and-white-collar-crimes.pdf.

COVER PHOTO ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**