CNAS

APRIL 2020

Emerging Threats in Combating Proliferation Finance

New Technology and Economic Challenges

Neil Bhatiya

America Competes

About the Author

NEIL BHATIYA is an Adjunct Fellow with the Energy, Economics & Security Program at the Center for a New American Security (CNAS). His work focuses on how the United States uses tools of coercive economic statecraft, including sanctions and investment and trade controls, to achieve foreign policy and national security goals. He also studies how sanctions impact the geopolitics of energy markets.

Before joining CNAS, he was the Climate and Diplomacy Fellow at the Center for Climate and Security. He was also previously a Fellow at The Century Foundation. His writing has appeared in *Foreign Policy*, World Politics Review, Bloomberg, *The Atlantic*, and *The Diplomat*.

Mr. Bhatiya received his MA in History from The George Washington University. He graduated from Marist College with a BA in History. Follow him on Twitter @NeilBhatiya.

Acknowledgments

I would like to thank Maura McCarthy and Melody Cook for their assistance with the drafting and production of this report. I also gratefully acknowledge Elizabeth Rosenberg, Yaya J. Fanusie, and Jonathan Brewer for their valuable ideas, encouragement, and feedback.

About the Energy, Economics & Security Program

The Energy, Economics & Security Program analyzes the changing global energy and economic landscape and its national security implications. From the shifting geopolitics of energy to tools of economic statecraft, such as trade policy and sanctions, the program develops strategies to help policymakers understand, anticipate, and respond. This program draws from the diverse expertise and backgrounds of its team and leverages other CNAS experts' strengths in regional knowledge, defense, and foreign policy to inform conversations in the nexus of energy markets, industry, and U.S. national security and economic policy.

America Competes

2020

America Competes 2020

America Competes 2020 is a Center-wide initiative featuring cutting-edge CNAS research, publications, events, and multimedia aimed at strengthening the United States' strategic advantages at home and abroad.

EMERGING THREATS IN COMBATING PROLIFERATION FINANCE

New Technology and Economic Challenges

Executive Summary

For decades, the United States, its allies, and partners have been policing the international financial system in an effort to deny the world's most dangerous weapons to the world's most dangerous actors. North Korea, Iran, Syria, and terrorist organizations such as the Islamic State group (ISIS) have, at various points, sought weapons of mass destruction (WMD) capabilities or their delivery systems. These actors have done so by moving illicit funds through the international financial system, exploiting an increasingly globalized world. Traditionally, efforts to combat this have focused on improving oversight of the global financial services industry and supply chains. Sanctions, export controls, and vigilance measures (customer checks and transaction monitoring) are essential to this effort.

Proliferation networks have frequently adapted in response, changing their methodologies to avoid detection. Increasingly, these networks are also embracing technological change. If the United States wishes to continue the policy leadership role it has adopted over the previous several years, it will need to understand how these networks are working to stymie the international community's efforts to discover and disrupt their activities.

Policymakers must prepare to more comprehensively tackle two emerging threats, which this paper will outline in turn. The first threat stems from proliferators' adoption of new financial technology, particularly their exploitation of platforms and payment systems designed to keep users and transactions anonymous or pseudonymous. North Korea, for example, has raised millions of dollars through the hacking of virtual currency exchanges. The second threat stems from new technology in the advanced manufacturing, chemical, and biological space, which can make advanced dual-use goods more accessible to more users; these technologies may also entail significant national security risks, especially in the hands of nation-state actors.

This paper recommends that the United States and its partners pursue policy adaptations across several lines. The United States should continue to raise awareness of specific proliferation finance issues by highlighting them in successive National Illicit Finance Strategies, including expanding their focus on illicit finance typologies arising from virtual currency use. The administration can best complement these efforts by drastically expanding its coordination with major economies on cybersecurity efforts to defend against advanced North Korean hacking capabilities.

The United States must also prioritize continuing partnerships between national governments around the world and companies so that the private sector is able to ensure the legitimate use of their technology. These partnerships have historically facilitated information-sharing; both sides must continue to emphasize this impulse to keep up with the new frontiers of financial and technological innovation that are lowering barriers to facilitating financial transfers or researching and developing new chemical or biological agents. Congress can help by implementing legislative changes that continue to enhance oversight of export regulations so the private sector handles potentially dual-use technologies appropriately.

Increasingly, weapons of mass destruction proliferation networks are embracing technological change.

The international community, led by the United States, needs to demonstrate a renewed sense of urgency in response to an evolving threat environment. This effort involves the long and hard work of building new rules, forging new international partnerships, and understanding dizzying technological change. The consequences of failure in this endeavor would be quite stark: the unchecked proliferation of weapons of mass destruction and their delivery systems.

Introduction

Despite the efforts of the international community, a variety of illicit actors continue to exploit the international financial system to provide resources, material, and know-how for clandestine weapons of mass destruction (WMD) programs. These networks, which specialize in what experts refer to as proliferation finance, continue to pioneer methods to move through the global financial system in a way that is difficult for even the most sophisticated and well-resourced international banks to detect.[1] Likewise, many nation-states struggle to police their own financial and commercial sectors, due to a lack of resources or political will. In recent months, U.S. authorities have targeted with legal action Chinese banks that were operating brazenly on behalf of North Korea and have sanctioned Iranian-linked companies in multiple countries that were trafficking in WMD-precursor goods for Iran.[2] These are but a few examples of how this works in practice.

North Korea remains the principal threat actor in this space and shows no signs of slowing its WMD and ballistic missile programs, despite Pyongyang and Washington's ongoing diplomacy. Iran had been trying to pressure the other parties to the Joint Comprehensive Plan of Action (JCPOA), also known as the Iran nuclear deal, to provide the economic relief to convince Tehran to continue complying with the deal.However, the Iranian leadership is currently testing the international community's patience by expanding its enrichment activities beyond the limits the JCPOA imposed. Other states such as Syria, as well as various non-state actors, including terrorist groups, continue to pursue WMD capabilities.[3] These actors represent a stark security threat for the international community.

The United States and its international partners have focused legal, regulatory, and intelligence resources on tracing these proliferation networks that operate through financial institutions around the world. Stronger implementation of export controls, sanctions, and other vigilance measures, such as customer due diligence, know-your-customer policies, and, for some jurisdictions, collection of beneficial ownership information, has been the center of that response.[4] If the United States wishes to continue the policy leadership role it has adopted over the previous several years, it will need to understand how these networks are adapting to the international community's efforts to discover and disrupt their activities.[5] None of these adversaries has been stagnant; they continue to learn new methodologies and find loopholes and have been especially adept at leveraging new technology.

Successive United Nations Panel of Experts reports and open source reporting and analysis have highlighted the creativity of the most sophisticated networks.[6] As the difficulty of doing illicit business in the United States and western Europe has increased, these networks are directing more of their activity to jurisdictions with less sophisticated legal and financial systems. Not only do these networks search out countries with weak financial crimes compliance frameworks, but they are also poised to exploit countries that are adding advanced manufacturing capabilities to their domestic economy. A recent example includes the U.S. sanctioning of an Iranian procurement network that was purchasing dual-use goods from China. In the past, these actors would have sought these goods from the United States or Europe.[7] Proliferation networks have always ridden the wave of expanding globalization; they will continue to do so.

Policymakers should pay attention to two emerging threats. The first is proliferators' adoption of new financial technology, particularly by exploiting platforms and

Despite the ongoing diplomatic process between the United States and North Korea, Pyongyang continues to augment its arsenal, including through testing missiles, like the one pictured. North Korea remains one of the world's most sophisticated exploiters of the international financial system to acquire these capabilities. (Woonhae Cho/Getty Images)

payment systems designed to keep users and transactions anonymous or pseudonymous. Bitcoin is only the most prominent of the cryptocurrencies that the international community and the United States have linked to North Korean and Iranian illicit activity.[8] There are several other cryptocurrency options that offer even greater ability to evade detection (for example, so-called privacy coins).[9] Also, there is a rise in efforts by sovereign states to create national cryptocurrencies, with prominent examples in Russia and Venezuela, both of which are motivated to evade U.S. sanctions exposure. While many of these efforts have been unsuccessful at their stated purpose, they are suggestive of the future prospects of alternative monetary products and value transfer systems, where the financial crimes compliance infrastructure needs to be much nimbler at responding to new typologies enabled by new financial technology (fintech), which include a wide array of methods designed to leverage digital means to compete with traditional financial services.

When the proliferators are not mining or trading virtual currency, they are stealing it outright, exploiting a digital finance environment where cybersecurity protections are uneven.

When the proliferators are not mining or trading virtual currency, they are stealing it outright, exploiting a digital finance environment where cybersecurity protections are uneven. As a result, it is growing easier to move money onward without touching U.S. jurisdiction, or outside of the view of many national regulators. The international community, as well as private sector firms innovating in this space, is in the early days of thinking through the proper regulatory responses. To be effective, this effort must include how to extend know-your-customer and customer due diligence protocols from the traditional financial space to this new technology realm, including answering questions about the notion of identity and jurisdictional reach. The responses must also focus on constantly strengthening a global cybersecurity posture that hardens cybersecurity infrastructure around virtual asset providers, to say nothing of those who transact in fiat currencies.

Second, international regulators and law enforcement must address threats from new technology in the advanced manufacturing, chemical, and biological space, which can make advanced dual-use goods more accessible to more users; these technologies may also entail significant national security risks, especially in the hands of nation-state actors. To respond to this, international regulators and their law enforcement counterparts must recognize that such innovations can rob the United States and its partners of their leverage in ensuring the responsible use of technology and materials with potentially harmful uses. Export controls are an important cornerstone of nonproliferation policy, but they may lose their utility in a world with radically democratized access to national security-sensitive technology, such as combinatorial chemistry and viral genome synthesis. The international control regime—the network of intergovernmental and private sector institutions that governs trade in dual-use goods—must be structured to confront this new reality and account for the accelerated pace of technological change.

The United States and its international partners have clear policy options at their disposal for addressing these security threats as they change over time. Previous innovations in countering proliferation finance have needed significant political will; budgetary resourcing has also been important. The international community, led by the United States, needs to demonstrate a renewed sense of urgency in response to an evolving threat environment.

Why the United States Has a Unique Role to Play

The ability of the United States to lead on countering illicit finance in general and combating proliferation finance specifically rests on a legal and regulatory framework that leverages its centrality in global finance and as a supply chain node.[10] The nature of the dollar-based finance and trading system, which provides the agreed-upon framework for a great deal of cross-border trade and investment, offers significant advantages to the sovereign issuer and controller of that currency.[11] By extension, that sovereign also holds significant influence over financial institutions, domestic and foreign. As described by academics Henry Farrell and Abraham L. Newman, "states with political authority over the central nodes in the international networked structures through which money, goods, and information travel are uniquely positioned to impose costs on others."[12] The United States has not hesitated to impose those costs on adversaries in pursuit of its foreign policy goals and, when done in a more multilateral setting, collective security objectives, like nonproliferation.

Though financial institutions around the world pay careful attention to the legal expectations set by their national regulators, ultimately those that are most concerned about their international business pay particular heed to the expectations U.S. regulators set. Though the Office of Foreign Assets Control (OFAC) is not a prudential regulatory agency per se, financial institutions around the world closely follow its guidance on sanctions compliance and its enforcement actions.[13]

This centrality of leadership is particularly true for what Treasury officials have referred to as "network sanctions" that target the "shell companies, business partners, facilitators, enablers, and middlemen to disguise the nature of their activity and launder their money." In August 2019, for example, the United States designated a Hong Kong-based company, Green Industries Limited, for its activities procuring dual-use goods.[14] The goods were purchased on behalf of Iran's Islamic Revolutionary Guards Corps (IRGC) for use in that country's ballistic missile work. The IRGC-linked network leaders used a company based in Hong Kong in large part to conceal that the goods were ultimately destined for Iran.

U.S. adversaries are responding to targeted financial sanctions, and these entities are an adaptation in their effort to prop-up proliferation finance networks.[15] The use of targeted financial sanctions is the traditional first step by national governments to deny resources to proliferation finance networks. The Financial Action Task Force (FATF), the international standard-setter for countering illicit finance efforts, uses implementation of these sanctions as its most important criteria for how nations deal with proliferation finance.[16]

The U.S. Treasury has consistently used sanctions to target complex fundraising networks for adversary regimes. President Donald Trump outlined this wider strategy against Iran at a January press conference. (Chip Somodevilla/Getty Images)

As a result of these efforts, however, proliferation networks engage in ever more elaborate use of shell and front entities to advance their illicit activity. Consequently, international banks find they need to do more extensive network analysis to look for evasion typologies. It is for this reason that the international community, including the FATF and the United States, have insisted that the private sector implement other vigilance measures in order for the countering proliferation finance regime to have any coherence.[17]

Creative U.S. leadership is critical at this time because the multilateral nature of counterproliferation efforts is straining under the growing tension around the United States' use of targeted financial sanctions. Many U.S. allies find the use of these tools, particularly against Russia and Iran, to be highly controversial. The

conversation on the use of these tools has shifted from disputes about specific foreign policy issues to a broader consideration of whether U.S. financial primacy should go unchallenged. The Obama and Trump administrations' use of sanctions has pushed mere complaints into efforts toward specific actions, though significant progress remains elusive.[18] Allies and partners are working to insulate themselves from the consequences of U.S. sanctions policy.[19] While the United States has long enjoyed an advantageous position in controlling these networks, there is nothing axiomatic about its dominant position. This resistance to U.S. sanctions policy has profound consequences for U.S. leadership on countering proliferation finance.

Proliferation networks engage in ever more elaborate use of shell and front entities to advance their illicit activity.

Some of these efforts, such as the European-backed Instrument in Support of Trade Exchanges (INSTEX), were meant to address sanctions issues around specific foreign policy controversies.[20] INSTEX and the French-proposed oil-backed credit line were designed to restore trade relations with Iran such that Tehran believed it was receiving economic benefits promised through compliance with the nuclear deal. U.S. sanctions targets have pursued creating sovereign cryptocurrencies: Venezuela has seen limited success (with the petro), and this is an idea various officials from Russia, China, and Iran have floated. Many sanctioned nation-states have pushed the idea of building an alternative to the global financial messaging service, SWIFT, which may include new financial technologies to transfer value using platforms that the United States cannot as easily track or interdict as with the traditional financial framework.[21]

None of these initiatives augurs a permanent move away from the U.S. dollar; the global private sector sees no other currency as a credible alternative for trade and investment. Even a modest decrease in its supremacy, however, poses challenges for U.S. leadership and its exploitation of those global network effects. As Farrell and Newman describe it:

> Targeted states—or states that fear they will be targeted—may attempt to isolate themselves from networks, look to turn network effects back on their more powerful adversaries, and even, under some circumstances, reshape networks so as to minimize their vulnerabilities or increase the vulnerabilities of others.[22]

The two emerging threats described in this paper are both potential avenues for failure of the countering proliferation finance regime within this wider strategic context. To prevent this, the United States needs to understand more comprehensively how these current and potential methods risk changing the fundamental characteristics of how proliferation finance networks operate. Many of these techniques and technologies are born out of legitimate commercial interests. However, as with many innovations, illicit actors will find ways to exploit them for their own purposes. To maintain a strong proliferation finance regime, the United States will need to lead the international community in understanding and responding to these threats.

New Financial Technology

While proliferation networks have long used illicit means to support weapons of mass destruction proliferation activities, in recent years some of the most significant threat actors in this space have pioneered the abuse of new financial technology—virtual currencies and distributed ledger technologies, among others—to move money around. This section will outline recent typologies, underscoring how significant North Korea's cyber capabilities are and highlighting the need for a more urgent and comprehensive approach to securing this new frontier of the financial services industry.

Since the 2009 advent of the virtual currency Bitcoin, the financial sector has been racing to understand the implications of a suite of new technologies to broaden financial access, more seamlessly conduct transfers of funds (especially cross-border), and, in some cases, conduct significant financial transactions outside of the control or surveillance of a central authority or in ways that support user anonymity.

While financial innovation will no doubt spur economic growth, particularly in areas that have been ill-served by more traditional financial services firms, it also comes with significant risks. The United States has already seen illicit actors including terrorists, money launderers, and drug dealers embrace digital spaces as an extension of their traditional activities.[23] As a percentage of overall activity, the use of these new payment mechanisms is still low (especially compared with how much is still done on a cash basis), but it is growing at an aggressive rate, while the governance response from the international community and individual jurisdictions has been slow to catch up.

By far the most sophisticated state proliferation actor, North Korea, is also the most sophisticated criminal state actor in the virtual currency space.[24] Its track record includes mining virtual currency, hacking virtual currency exchanges, and demanding virtual currency payments as ransom for data stolen during cyberintrusions around the world.[25]

Since Bitcoin, one of the world's most prominent virtual currencies, came onto the scene, experts acknowledge its attractiveness to illicit actors such as North Korea: Bitcoin has a large market share, which means Pyongyang can target a wide community of users for its hacking activity. While exact numbers on how much North Korea has made as profit from Bitcoin remain hard to pin down, the overall transaction volumes remain quite high, with the United Nations suggesting a top-end estimate of over $100 million from 2017 to 2019.[26] Regardless of the specific amount, North Korea's use of this technology is proving to be a formidable threat.

In addition to virtual currency, there are other financial technology instruments that promise to introduce further innovation into global commerce but also represent opportunities for exploitation. Private sector interest is driving a great deal of the change, as these methods promise less expensive and more efficient payment systems when compared with traditional financial institutions. The promise of lower costs for more information is driving a lot of the innovation in this space: many of these technologies are built on distributed ledger technology, which is a way of decentralizing the collection of data. With distributed ledger technology, a record of transactions can be stored and verified through the consensus of a network's users, rather than through a central data-collection or settlement authority. In the shipping sector, operators are exploring how to use blockchain, an example of distributed ledger technology that records and verifies transactions in cryptographically secured sections called blocks.[27] The trade finance space, which requires bank intermediaries to verify the parties to trade transactions, is also open to such innovation, particularly as peer-to-peer transfers grow in popularity.[28]

As with virtual currency innovations, illicit actors are also exploring how to leverage other new technology instruments. The March 2019 United Nations Panel of Experts report highlighted the case of Marine Chain Platform Ltd., a Hong Kong-registered platform for ownership of maritime vessels that was based on blockchain technologies: the platform would allow users to buy and

Recent reports published by the United Nations have focused sustained attention on the extent to which North Korea is increasing its use of virtual currency to raise and move money. (Getty)

sell shares of vessels as tokenized assets.[29] Its creators may have been trying to exploit weaknesses identified by the Financial Stability Board, an international body created by the G20 to analyze the integrity of the global financial system. The board's June 2019 report on decentralized finance highlighted that the diffuse nature of the participants in these types of ventures means that the system of rules governing it is also diffuse. There is a lack of consensus on the laws that govern different parts of the transaction chain.[30] The Marine Chain case also points to how common cryptocurrency scams are, underscoring the poor regulatory environment.[31]

A strong financial crimes compliance approach by national monetary authorities and central banks needs to be accompanied by a strong cybersecurity response.

The international community, national-level regulators, and the firms operating in this sector need to respond to the broad suite of proliferators' technological capabilities with a far more unified approach than has been the status quo; otherwise proliferators will continue to use it to raise revenue to finance further developments in their weapons programs. They will also require expertise beyond the traditional sphere of financial crimes compliance. The response to fintech developments has been the responsibility of various public-private partnerships and aggressive action by particular central banks or monetary authorities. Moreover, the U.S. government asserts that the financial technology industry can and must comport itself in the same way the traditional financial services industry does when it comes to anti-money laundering (AML) and countering terrorist and proliferation financing. Often, the virtual currency purveyors themselves are taking the lead in trying to establish minimum standards for responsible players in this new space.[32]

These welcome developments are not enough. A strong financial crimes compliance approach by national monetary authorities and central banks needs to be accompanied by a strong cybersecurity response. The rise of virtual currencies has been met with a sophisticated cyberhacking and cybercrime campaign against the international community. This cyberthreat to new financial technologies exists alongside North Korea's ability to hack traditional financial services providers, including central banks.[33]

The United States and the Financial Action Task Force have both prioritized updating the financial regulatory structure to incorporate threats from the exploitation of new financial technology. Three relatively recent documents, published by international organizations and countries themselves, provide some initial direction for private sector actors about their legal and regulatory responsibilities to ensure illicit actors do not abuse these new payment platforms. These documents do have real-world impact. For example, after the FATF published its guidance on virtual assets, exchanges such as South Korea's Upbit chose to remove privacy coins from the exchange's offerings of digital tokens, since privacy coins are designed to obfuscate the users sending and receiving the currency in question (in contrast to non-privacy coins such as Bitcoin, where the wallet addresses and transaction histories of senders and receivers are visible).[34]

These 2018–2020 guidance documents, which provide much-needed context for other governments and the private sector to understand the threats they face, include:

- Successive U.S. National Illicit Finance Strategies (2018 and 2020) and the three supporting risk assessments (for countering terrorist financing, countering proliferation finance, and anti-money laundering efforts, published alongside the 2018 version). The anti-money laundering risk assessment in particular underscores virtual currency as a vector for abuse: "Virtual currencies, when exchanger and administrators are unregulated, also provide anonymity and pose risks due to the speed they can be transmitted, disintermediation, global reach, and the lack of regulation and supervision in many jurisdictions."[35]
- The Financial Crimes Enforcement Network (FinCEN) Guidance—Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 2019). The FinCEN Guidance does not specifically create new regulations; it merely seeks to remind those who may be operating as money transmitters in the convertible virtual currency space of their specific obligations under the Bank Secrecy Act, including as it pertains to AML requirements, and obligations around suspicious activity and currency transaction reporting (SARs/CTRs).[36]
- The FATF—Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019). Similar to the FinCEN Guidance, it emphasizes that existing FATF recommendations around anti-money laundering/countering terrorist financing apply to specific categories of virtual asset

service providers. Ultimately member states are responsible for the implementation of a legal and regulatory framework around these obligations, against which FATF will judge in its mutual evaluation reviews.[37]

The information, definitions, and guidance enshrined in these documents can be broken down thematically:

- Defining a universe of illicit activity that virtual currency users could engage in
- Defining what is a "business" that may be subject to specific regulations
- Setting up mechanisms of information-sharing between the public and private sectors to study how regulations can avoid stifling legitimate industry innovation

In addition to issuing guidance, many states have begun to update their legal frameworks in the face of this changing threat. Singapore's Payment Services Act provides for a licensing and regulatory regime for virtual currency providers, including allowing the government of Singapore, through its Monetary Authority, to designate what constitutes a "significant" payment systems operator, which will make it subject to more comprehensive regulations (the definition of significant being a function of a monthly average of payment transactions).[38] The law, which went into effect at the end of January 2020, also allows the Monetary Authority to mandate standards for cybersecurity protocols, in an effort to reduce the susceptibility of virtual asset providers to cyberattacks. Singapore is taking advantage of lessons learned through a carefully structured regulatory approach, which allows other firms to sell new financial services with relaxed legal requirements for a specifically delineated amount of time (though this does not relieve them of anti-money laundering or countering terrorist financing requirements).[39]

To date, there have been no documented cases of a proliferation actor using virtual currency to obtain a proliferation-sensitive good. The U.S. National Proliferation Financing Risk Assessment, for example, does not refer to the use of virtual currencies by proliferators, focusing more attention on the vulnerability of traditional financial mechanisms to exploitation. The lack of such a focus at this stage is understandable: because proliferators are looking for goods from reputable manufacturers, they are happy to default to using traditional mechanisms, such as open account transfers or trade financing, to acquire them. The attempted use of a virtual currency to buy high-density steel, for example, would raise far too many red flags to be a practical typology of proliferation financing. However, every day these actors become more proficient in using virtual currency to raise and move money, and they may one day be able to do more, especially as the use of these new payment mechanisms becomes more mainstream.

As a result, policymakers need to substantially accelerate their efforts to understand this threat. Several states of proliferation concern are using virtual currency as means to evade sanctions and move money around. The United States considers any overseas revenue raised by states such as North Korea, for example, to be in service of its military spending priorities, so Pyongyang's use of virtual currencies is implicated in a much broader definition of proliferation finance.

Every day proliferation actors become more proficient in using virtual currency to raise and move money, and they may one day be able to do more.

Individual countries must complement international principles with specific regulations and legislation at the national level. The FATF has only this year made it clear how it expects its member-states to apply counter illicit finance strategies to the virtual currency sector, including by requiring service providers collect sender/recipient information for virtual currency transfers over a certain monetary threshold.[40] This new guidance will likely spur an ongoing effort that will see repeats of previous disagreements between the public and private sectors about who is responsible for collecting and sharing data, what is reasonable under the law to expect from even large financial institutions, and how stringently each jurisdiction plans to enforce its laws.

A compliance effort on its own is insufficient, however. A regime for countering illicit finance must be matched by an effort to augment cybersecurity protections so that state-sponsored hacking is much less able to steal swiftly such large sums of money. Such an effort would require the public and private sectors to make significant resourcing and prioritization decisions around it, as well as coordinate closely among and between each other. This would be an opportunity for the United States to leverage its network centrality to improve global standards.

New Commercial Advances

While new financial technology, such as virtual currency, represents a new avenue for proliferation networks to raise money in a less well-regulated environment, there is an analogue with the avenues for evading or eroding export controls. These measures, designed to keep dangerous dual-use goods away from potentially dangerous purchasers, rest on the idea that the best technology for weapons of mass destruction program production originate in the United States and western Europe. As this section makes clear, however, many researchers and private companies are lowering the barriers to entry for many of these technologies. While many of the existing multilateral export control regimes, such as the Australia Group, an international organization that helps its member-states harmonize export controls, have begun to deal with this issue, they have not done so with the urgency that would require countries to keep up with the aggressive pace of change.

As referenced in Office of the Director of National Intelligence Worldwide Threat Assessments, the U.S. intelligence community is particularly concerned about the general ability of adversaries to manufacture advanced components with inexpensive technology and the potential military dimensions of specific advances in chemical and biological technology.[41] The fear is that many of these technologies, as the National Intelligence Council concluded, "will also lower the threshold for new actors to acquire WMD capabilities."[42]

The first concern is technologies such as three-dimensional printing. The second includes advances in synthetic biology, chemical synthesis, and nanobiotechnology, to name just a few, which could allow for the easier production of standard chemical or biological agents, or, less probably, the creation of novel agents with a substantially lower risk of detection by the international community.[43] Both instances present a challenge to the current approach to constraining the production of chemical and biological weapons. In contrast with much of the nuclear field (civilian and military), this space is relatively underprioritized outside of specific instances such as Syria's battlefield use of chemical weapons, or Russia's and North Korea's use of chemical agents to conduct targeted assassination of regime opponents. As a result, the international community has not built up the same robust level of controls and global governance.

Another challenge rests in the relative complacency about how easy it is to gain access to these technologies. In most cases, these technologies support applications in sectors requiring sophisticated knowledge by a wide range of highly educated individuals with specialized training and institutional-level support. This naturally limits the individual's usefulness for so-called lone wolf actors or small extremist groups. There is a much higher likelihood that states with weapons of mass destruction programs, either declared or covert, would find

FBI Director Christopher Wray and other top-ranking officials in the intelligence community have highlighted the potential military dimensions of the advent of new technologies that are lowering the barriers to entry for making novel chemical and biological compounds. (Win McNamee/Getty Images)

a particular technology useful.[44] The issue is that, as technology advances, the threshold of skills needed (on a relative basis) to produce dangerous materials decreases marginally. And, as the diffusion of new technologies increases, traditional export controls decline in effectiveness. With more new entrants into market, the number of entities and jurisdictions the international community needs to monitor grows and raises questions about whether the rules are adequate to the new reality.

Recently, however, national security policymakers have begun to try to sound more specific warnings about specific technologies. For example, in first highlighting the threat of relatively inexpensive gene editing technology in congressional testimony, then-Director of National Intelligence James Clapper stated that "Given the broad distribution, low cost, and accelerated pace of development of this dual-use technology, its deliberate or unintentional misuse might lead to far-reaching economic and national security implications."[45] Part of a comprehensive risk assessment of these changes begins with an understanding of which particular actors will find these new technologies practical for their purposes.

As technology advances, the threshold of skills needed (on a relative basis) to produce dangerous materials decreases marginally.

In a landmark study for the Defense Threat Reduction Agency, a group of researchers put together a framework for understanding which technologies were most worrisome from an accessibility, ease of use, and governance perspective—in other words, how likely was it that current control regimes could adequately respond to the ability of even unsophisticated actors to access these technologies for illicit or dangerous uses. Of the ones they analyzed, among the highest risk were:

- Combinatorial chemistry and high-throughput screening: These two related techniques are used to create, through the former, thousands of new combinations of molecules to discover entirely new chemical compounds, and, through the latter, screen them for specific biological characteristics. The commercial prospects are strongest for new medicines and pesticides—it becomes easy to develop new compounds and test them for lethality to other living organisms (humans or livestock). Whereas a commercial actor would dismiss too-lethal compounds as not commercially viable, a proliferation actor would be using the technology specifically to achieve such an outcome.[46]
- Chemical microprocess technology: These devices represent a generational improvement over traditional batch reactors for chemical agents. With more sophisticated computer-assisted monitoring, the microprocessors can generate highly corrosive compounds at higher "quality, quantity, and rapidity of reactions." Such technology could overcome one of the biggest obstacles to generating significant quantities of chemical agents, which are easy to create in small quantities but become substantially difficult for actors who want enough quantity of a compound to use as a weapon.[47]
- Synthesis of viral genomes: The technology to engineer DNA sequences to create synthetic genes has existed since the 1970s, while the ability to "build" viral genomes dates back to the early 2000s. While some have speculated that such technology could be used to create entirely new viruses, most experts find that unlikely.[48] Rather, most well-resourced and sophisticated nation-state-directed programs would be most adept at creating well-known, but no less dangerous, viral pathogens.
- DNA shuffling and directed evolution: These related technologies involve the manipulation, through the introduction of chemicals, of the underlying genetic makeup of an organism to change its basic characteristics. Experiments with such techniques have allowed the creation of viruses that can affect species in way that would not have been possible in nature. Among the concerns cited by researchers is that such manipulation could increase an organism's resistance to antibiotics.[49] These concerns are similar to those raised by CRISPR (clustered regularly interspace short palindromic repeats) gene editing, which has come into much higher profile since the study was released.

China's innovations in many of these technologies worry U.S. policymakers, especially as Beijing seeks to build connections to obtain advanced military technology from other countries.[50] Chinese military sources have repeatedly referenced the military utility of genetic editing.[51] While China does not have a track record of onward proliferation of such technologies, and indeed it would be in its interest to prevent these methods from

spreading beyond its borders, U.S. policymakers should not rule out situations where such weapons could be provided to allies in specific circumstances, including by disloyal insiders operating on their own account. There is the ever-present possibility of rogue elements selling or giving away the know-how independent of Beijing's desire that such an eventuality not occur.

More concerning than the ability of any one technology to be of immediate use to a malign actor is the fact that the internal control regime is slow to adapt to the pace of new technologies. The prospect that the non-state actor may be able to obtain and wield these technologies with the same skill as a state actor would represent a significant obstacle for combating proliferation networks. The entire foundation of the present system of financial controls on illicit procurement rests on the idea that it is possible to surveil transactions and trade flows between the manufacturing sites for these items and the locations of proliferating states or groups. Such technologies could, as they continue to advance, erase that leverage.

Currently, the international community and the United States have instruments to try to address the implication of new technologies for nonproliferation priorities.[52] Advances in chemical and biological weapons are both governed by international conventions. However, as has been noted by many other analysts, these conventions often lack significantly coercive enforcement mechanisms. Additionally, the need for consensus and the infrequency of the review conference meetings often mean that the conventions are slow to keep up with new technology.

An additional weakness is that, as with many control regimes for a variety of proliferation-specific goods or technology, states and organizations enforcing the norms of nonproliferation tend to focus on states that are already understood by the international community to be ones of proliferation concern. This means that states that are not already high-risk could conceivably take at least the initial steps to build a program for developing weapons of mass destruction because they are not being closely monitored. Additionally, sophisticated non-state actors or individuals represent a more difficult threat to track, though their efforts have been limited by scaling-up challenges.[53]

The United States should move aggressively to address these shortcomings. It should do so by leveraging its close relationships with the implementing agencies of the Chemical Weapons Convention and the Biological Weapons Convention. The United States maintains a great deal of credibility within both conventions, having worked closely with the implementation agency of the Chemical Weapons Convention, the Organisation for the Prohibition of Chemical Weapons (OPCW), to nearly eliminate Syria's chemical weapons stockpile.[54] Similarly, the Biological Weapons Convention represents another forum for policy innovation. In each circumstance, the United States must stress the dangers of complacency. It has acted similarly in the nuclear field. It must also do so for a variety of next-generation technologies, many of which are hard to foresee.

In recent years, actions by states such as Russia and Syria have eroded the taboo around the use of chemical weapons. The capability to deploy agents such as Novichok, which killed four United Kingdom residents in two separate incidents, may be more accessible for a wider array of actors. (Jack Taylor/Getty Images)

Recommendations

The following policy recommendations focus on actions the U.S. government and Congress should consider to adapt the countering proliferation finance regime to a new suite of threats, including changing economic circumstances and new financial and commercial technologies that can make it easier for proliferation actors to move money around or acquire potentially lethal dual-use goods.

The United States has a strong record on leading the international community on broad counterproliferation policy. Adopting these recommendations represents an opportunity to build on that work, making the regime stronger, more nimble, and more ready to face over-the-horizon challenges.

Recommendations for the Executive Branch

- *Augment the National Illicit Finance Strategy to include fintech.* The National Illicit Finance Strategy and risk assessments are important documents for signaling priorities to the financial sector and setting the stage for the Treasury Department's international engagements. The department should continue to include a strong focus on virtual currency in its national illicit finance strategy and the risk assessments for anti-money laundering, countering terrorist financing, and countering proliferation finance risk assessments. A variety of illicit finance actors in each of these three risk categories will continue to use virtual currency. Over time, the Treasury Department should considering publishing a separate one for the entirety of the virtual currency sector. A separate document would address the unique needs of the sector as it continues to expand and respond to the newly issued regulations of multiple jurisdictions, including in response to the new Financial Action Task Force guidance. This new publication would help Treasury coordinate with the Federal Reserve and state-level regulators about the broader macroeconomic context for the increased use of virtual currency.
- *Reinforce existing work on proliferation finance at the Financial Action Task Force.* The Treasury Department should make the most of China's presidency of the Financial Action Task Force to encourage its effort to address countering the financing of proliferation generally, and efforts to improve oversight of virtual assets in order to combat this sector's exploitation by illicit financial actors. The Financial Action Task Force under the United States undertook this effort in a serious way, including through the convening of a working group specifically focused on countering proliferation; it should be important for the United States to encourage member-states to continue it.
- *Expand efforts to deal with cyber-related issues.* The United States and like-minded member states should convene a FATF working group on financial institution cybersecurity. The working group should start with a global risk assessment on cybersecurity. This government-run effort should complement efforts by the private sector to constantly improve industry standards, working with their national authorities. This working group should take a balanced approach, focusing on threat actors in both the virtual currency and traditional financial services sectors.
- *Improve how Central Banks approach cybersecurity.* The U.S. Department of State should lead at the G20 on a central bank cybersecurity initiative. This newly created effort would coordinate on risk assessments, identifying best practices for shielding central banks from cyber-based intrusions, and sharing typologies. This effort would complement efforts by the G20 to coordinate a working group on new financial technology.
- *Strengthen bilateral cooperation with partner nations.* The Department of the Treasury, the Department of Homeland Security, and U.S. Cyber Command should prioritize efforts to help U.S. partner nations augment their cybersecurity defense against state-sponsored hacking. These efforts should focus in particular on protecting computer systems associated with financial institutions, including virtual currency providers.
- *Improve regulatory harmonization for fintech.* The Treasury Department should leverage the full suite of multilateral forums that the United States actively participates in to make the case for close coordination on the adoption of regulations in the financial technology space. This effort would complement bilateral engagement with important financial jurisdictions such as London, Frankfurt, Singapore, Hong Kong, and Seoul.
- *Ensure a comprehensive legislative framework for Export controls and new commercial technologies.* As the Commerce Department continues to explore how to implement the Export Control and Reform Act of 2018 (ECRA), it should pay close attention that its definitions of emerging technologies include a particular focus on new manufacturing, biological, and chemical methods that have implications for weapons of mass destruction proliferation.

The U.S. government has increased its regulatory scrutiny of virtual currencies such as Bitcoin, whose futures are being traded in exchanges like the one pictured in Chicago. (Scott Olson/Getty Images)

- *Have more focused discussions on updating the Chemical Weapons Convention and the Biological Weapons Convention.* The U.S. State Department, in its delegation activities within the Chemical Weapons Convention and Biological Weapons Convention, should encourage more regular meetings of committees focused on monitoring research and development activities and help focus member states on consistent implementation.
- *Engage with the Australia Group.* The U.S. State Department, in its delegation activities within the Australia Group, should encourage that body to make permanent its ad hoc working committees on emerging technologies so there can be a more unified global effort to harmonize approaches to dual-use goods.
- *Explore new international conventions.* The National Security Council should conduct an interagency assessment of whether additional framework conventions are needed to address specific emerging technologies that, in the estimation of relevant agencies, are not adequately addressed by the existing arrangement of control groups.

Recommendations for Congress

- *Create a Virtual Currency Task Force/Study Group.* Recent hearings, especially on Facebook's proposed Libra virtual currency, highlight the important role Congress has in overseeing how the private sector innovates in this space. To better organize these efforts, Congress should authorize and fund a Virtual Currency Task Force, whose mandate would be to analyze the impact of existing and pending legislation on the fintech industry. Such a task force would help guide Congress in taking a careful regulatory posture with respect to financial technology.
- *Provide strong oversight of the implementation of the ECRA and the Foreign Investment Risk Review Modernization Act (FIRRMA).* Congress, through regular oversight hearings, should pay close attention the administration's implementation of ECRA. Relevant committees should oversee how the Treasury and Commerce departments finalize regulations and should pay close attention to the security implications of emerging dual-use technologies. Congress should actively pursue testimony from relevant private sector actors.
- *Augment U.S. analysis of private sector research and development efforts.* Congress should provide additional funding to the National Academy of Sciences and the federal research laboratories to dedicate more effort to understanding new technology applications in the chemical and biological space, with a special focus on potential dual-use violations and technologies vulnerable to weaponization.

Recommendations for the Private Sector

- *Explore new methodologies for data-sharing focused on new financial technology.* In addition to responsible engagement with government entities on developing compliance expectations for the fintech industry regarding know-your-customer and customer due diligence, the fintech industry should also explore voluntary data-sharing mechanisms to combat illicit finance, reflecting the legal requirements and restrictions of their respective jurisdictions. Such a mechanism could include sharing of anonymized typologies of illicit actors in the fintech space, which the industry could compile and share privately with relevant financial intelligence units or law enforcement agencies. Over time, this effort could include these firms forming a regular public-private body that would meet periodically so industry could learn from government and vice versa.
- *Engage with the administration and Congress on FIRRMA and ECRA implementation.* While the administration works to provide the regulatory framework to implement these new laws, the private sector should embrace as many opportunities as possible to engage in the rulemaking process. Industries that research and produce potential dual-use goods should pay attention to how the markets they operate in could be exploited by proliferation actors.
- *Review the prospects for voluntary sharing of best practices in dual-use controls.* The private sector should assess the feasibility of augmenting existing (or creating entirely new) voluntary associations governing new developments in advanced manufacturing, chemical, and biological technologies. Industry associations should habitually share best practices on the responsible selling of such goods, particularly in the space of knowing-their-customers. There is an oft-cited lack of coordination between the manufacturing sectors and financial sectors on how to address these issues in a systemic way; such associations should also explore what dialogue mechanisms may be appropriate to address this shortcoming.

Conclusion

Even if only some of the risks outlined in this paper come to pass, they will pose dangerous challenges to the countering illicit finance regime in general and the countering proliferation finance regime specifically. Marginal adoption of new financial technology by proliferators will make it easier for them to move money around—especially if they are able to steal virtual currency from exchanges or wallet providers that lag dangerously behind in adopting the latest cybersecurity standards. Additionally, there are many potential breakthroughs in the advanced manufacturing, chemical, and biological space that could make it substantially easier for even a modestly resourced state-sponsored program to obtain and maintain a significant arsenal of weapons. These innovations may also be inexpensive and obtainable enough for non-state actors, including terrorist groups or "lone wolf" extremists, to wield.

The proliferation finance environment is a constantly changing one, but policymakers have many tools and best practices at their disposal to coordinate a significantly stronger response. As stated in previous Center for a New American Security (CNAS) reports, there is no insuperable obstacle to designing a better countering proliferation finance regime; what is required is the political will to continually invest in stronger policy response and implementation, and to push large institutions to innovate as adeptly as the illicit actors they are trying to disrupt.

The economic and technological threats outlined in this report should be at the top of any responsible jurisdiction's priority list. The first threat is advances in financial technology, particularly the growing mainstream use of virtual currencies, which presents another vector through which proliferation networks can hide and move financial resources. The second threat is how these actors will continue to explore how advanced manufacturing, particularly as it relates to chemical and biological research, development, and production, will make sophisticated capabilities more easily accessible.

It is important not to exaggerate the impact of any one of these new developments. By themselves, they do not represent a radical change in the ability of state or non-state actors to obtain WMD capabilities or the resources to obtain them. However, taken together, they do pose an opportunity for U.S. adversaries to augment their capabilities in a way that is much harder for the United States and its partners in the international community to counteract. Many of these challenges have been building for years; it will similarly take years-long efforts to address them in a vigorous way.

Fortunately, it is not incumbent on the international community to invent entirely new tools to deal with this evolving challenge. The United States is uniquely influential, by virtue of the predominant role of the U.S. dollar in world trade and investment, in setting global standards for measures to be taken by states and by financial institutions to mitigate risk of proliferation finance. Responsible states and their private sector actors have long recognized at least some responsibility to find ways to fight these malign actors. Countries that wish to meet these threats head-on need to invest in updating those laws, regulations, and agencies to meet the dilemmas presented by 21st century proliferators. The United States should provide encouragement and support. The costs of not doing so (or doing so in a way that is likely to lead to failure) could be clearly catastrophic, for the United States as well as the international community as a whole.

Endnotes

1. See additional CNAS reports on combating the financing of WMD proliferation: Elizabeth Rosenberg, Neil Bhatiya, Claire Groden, and Ashley Feng, "Financial Networks of Mass Destruction," (Center for a New American Security, January 30, 2019), https://www.cnas.org/publications/reports/financial-networks-of-mass-destruction; and Jonathan Brewer, "The Financing of WMD Proliferation" (Center for a New American Security, October 30, 2018), https://www.cnas.org/publications/reports/the-financing-of-wmd-proliferation.

2. "U.S. appeals court upholds ruling against Chinese banks in North Korea sanctions probe," Reuters, July 30, 2019, https://www.reuters.com/article/us-usa-trade-china-banks/us-appeals-court-upholds-ruling-against-chinese-banks-in-north-korea-sanctions-probe-idUSKCN1UQ03U; and "Treasury Sanctions Global Iranian Nuclear Enrichment Network," U.S. Department of the Treasury, press release, July 18, 2019, https://home.treasury.gov/news/press-releases/sm736.

3. Daniel R. Coats, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record to the Select Committee on Intelligence, U.S. Senate, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

4. For a description of how these policies fit together, see Sohail Akbar, "How to Audit Know Your Customer (KYC) and Customer Due Diligence (CDD)," (Association of Certified Anti-Money Laundering Specialists, October 2018), http://files.acams.org/pdfs/2019/Sohail-Akbar-White-Paper.pdf.

5. For a review of U.S. priorities at the Financial Action Task Force, see "Objectives for FATF-XXX (2018-2019)," Financial Action Task Force, http://www.fatf-gafi.org/media/fatf/content/images/Objectives-FATF-XXX-(2018-2019).pdf.

6. "Midterm report of the Panel of Experts established pursuant to resolution 1874 (2009)," (United Nations Security Council, August 2019), https://undocs.org/S/2019/691; Lucas Kuo and Jason Arterburn, "Lux and Loaded: Exposing North Korea's Strategic Procurement Networks," (C4ADS, July 2019), https://www.c4reports.org/lux-and-loaded; and Andrea Berger and Anagha Joshi, "Countering Proliferation Finance: Implementation Guide and Model Law for Governments," (Royal United Services Institute, July 21, 2017), https://rusi.org/publication/other-publications/countering-proliferation-finance-implementation-guide-and-model-law-0.

7. "U.S. sanctions network selling materials for Iran nuclear program," Reuters, July 18, 2019, https://www.reuters.com/article/us-mideast-iran-usa-sanctions/u-s-sanctions-network-selling-materials-for-iran-nuclear-program-idUSKCN1UD2PV.

8. "Midterm report of the Panel of Experts established pursuant to resolution 1874 (2009)."

9. Privacy coins offer different protocols for disguising the digital identities, amounts, and locations for virtual currency holders and transactions. Many exchanges have rejected the presence of privacy coins, fearing that criminal actors may be using them to avoid anti-money laundering checks. Will Heasman, "Privacy Coins in 2019: True Financial Freedom or a Criminal's Delight?," CoinTelegraph.com, January 2, 2020, https://cointelegraph.com/news/privacy-coins-in-2019-true-financial-freedom-or-a-criminals-delight.

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

11. Peter Harrell and Elizabeth Rosenberg, "Economic Dominance, Financial Technology, and the Future of U.S. Economic Coercion," (Center for a New American Security, April 2019), https://www.cnas.org/publications/reports/economic-dominance-financial-technology-and-the-future-of-u-s-economic-coercion.

12. Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security*, 44 no. 1 (Summer 2019), 45.

13. In a recent survey about perceptions of proliferation finance risk, U.S. government documents ranked only behind Financial Action Task Force guidance when it came to important sources of information for compliance and other private sector officials who are responsible for managing risk in their institutions. Emil Dall and Justine Walker, "RUSI-ACAMS Proliferation Finance Survey," (Royal United Services Institute and the Association of Certified Anti-Money Laundering Specialists, February 5, 2020), http://files.acams.org/pdfs/2020/ADT175_ACAMS_RUSI-Survey-Report-Documentation.pdf. The Office of Foreign Assets Control's document titled *A Framework for OFAC Compliance Commitments* is only among the most recent guidance from OFAC that tells financial institutions where they typically fall short of what a sound compliance program looks like. U.S. Department of the Treasury, *A Framework for OFAC Compliance Commitments* (May 2, 2019), https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.

14. "Treasury Sanctions Global Iranian Nuclear Enrichment Network."

15. See recommendation 7 in "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," (Financial Action Task Force, 2012, updated June 2019), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

16. Consolidated assessment ratings for all of the Financial Action Task Force recommendations can be found at Financial Action Task Force, "Consolidated assessment ratings," https://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html.

17. Financial Action Task Force, "FATF Guidance on Counter Proliferation Financing," (February 2018), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf.

18. For number of designations, see Gibson Dunn, "2018 Year-End Sanctions Update," February 11, 2019, https://www.gibsondunn.com/2018-year-end-sanctions-update/. For a discussion of how the efforts of U.S. partners such as Europe to innovate their ways around U.S. sanctions are spurring larger conversations about the primacy of the U.S.-led financial and economic system, see Jean Pisani-Ferry, Mark Leonard, Elina Ribakova, Jeremy Shapiro, and Guntram Wolff, "Redefining Europe's economic sovereignty," (European Council on Foreign Relations, June 25, 2019), https://www.ecfr.eu/publications/summary/redefining_europes_economic_sovereignty.

19. Farrell and Newman, "Weaponized Interdependence," 76.

20. Deborah Amos, "How Instex, Europe's Trade Channel with Iran, Will Work," NPR, July 5, 2019, https://www.npr.org/2019/07/05/739052023/how-instex-europes-trade-channel-with-iran-will-work.

21. Yaya Fanusie and Trevor Logan, "Crypto Rogues: U.S. State Adversaries Seeking Blockchain Sanctions Resistance," (Foundation for Defense of Democracies, July 2019), https://www.fdd.org/analysis/2019/07/11/crypto-rogues/.

22. Farrell and Newman, "Weaponized Interdependence," 76.

23. Edoardo Saravalle and Elizabeth Rosenberg, "Bitcoin can help terrorists secretly fund their deadly attacks," Fox News, January 9, 2018, https://www.foxnews.com/opinion/bitcoin-can-help-terrorists-secretly-fund-their-deadly-attacks.

24. David Carlisle and Kayla Izenman, "Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia," (Royal United Services Institute, April 14, 2019), https://rusi.org/publication/occasional-papers/closing-crypto-gap-guidance-countering-north-korean-cryptocurrency.

25. The wide scale and breadth of North Korean activity can be seen chiefly in the August 2019 report of the United Nations Panel of Experts on North Korea. The panel's regular reports on sanctions enforcement remain one of the single best sources for case studies of North Korean sanctions evasion, including the increasingly sophisticated use of virtual currencies to move money around the international financial system. "Midterm report of the Panel of Experts established pursuant to resolution 1874 (2009)."

26. Midterm report of the Panel of Experts established pursuant to resolution 1874 (2009), 111-112.

27. Keith Johnson and Elias Groll, "U.S. Sanctions Weapon Is Under Threat—but Not From Bitcoin," *Foreign Policy* (January 24, 2018), https://foreignpolicy.com/2018/01/24/u-s-sanctions-weapon-under-threat-but-not-from-bitcoin-blockchain-dlt-petro/.

28. Helen Partz, "Major Singapore Bank Completes First DLT Trade Financing Transaction," CoinTelegraph.com, October 17, 2019, https://cointelegraph.com/news/major-singapore-bank-completes-first-dlt-trade-financing-transaction.

29. Cristina Rotaru, "The Curious Case of Marine Chain: The DPRK cyberscam behind a blockchain-powered maritime investment marketplace," Vertic, April 24, 2019, http://www.vertic.org/2019/04/24/the-curious-case-of-marine-chain-the-dprk-cyberscam-behind-a-blockchain-powered-maritime-investment-marketplace/.

30. "Decentralised financial technologies: Report on financial stability, regulatory and governance implications," (Financial Stability Board, June 6, 2019), 18, https://www.fsb.org/wp-content/uploads/P060619.pdf.

31. Ana Alexandre, "New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams," CoinTelegraph.com, July 13, 2018, https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams.

32. Global Digital Finance, for example, is an industry association that requires its members to adhere to specific principles across product categories and regulatory responsibilities, including know-your-customer and anti-money laundering efforts. Global Digital Finance, "Code of Conduct, Part VIII: Principles for KYC/AML," n.d., https://www.gdf.io/gdfcode/.

33. Carlisle and Izenman, "Closing the Crypto Gap," 9, 31-32.

34. William Foxley, "South Korea's Upbit Becomes Latest Exchange to Delist Privacy Coins," CoinDesk.com, September 20, 2019, https://www.coindesk.com/south-koreas-upbit-becomes-latest-exchange-to-delist-privacy-cryptocurrencies. For more detail on privacy coins, see Olga Kharif, "Privacy Coins Face Existential Threat Amid Regulatory Pinch," Bloomberg, September 19, 2019, https://www.bloomberg.com/news/articles/2019-09-19/privacy-coins-face-existential-threat-amid-regulatory-crackdown.

35. "National Illicit Finance Strategy," (U.S. Department of-gov/system/files/136/nationalstrategyforcombatingterroristandotherillicitfinancing.pdf; and "National Strategy for Combating Terrorist and Other Illicit Financing: 2020." For the accompanying risk assessments for the 2018 strategy, see "National Terrorist Financing Risk Assessment," (U.S. Department of the Treasury, December 20, 2018), https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf; for proliferation financing: "National Proliferation Financing Risk Assessment," (U.S. Department of the Treasury, December 20, 2018), https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf; and anti-money laundering: "National Money Laundering Risk Assessment," (U.S. Department of the Treasury, December 20, 2018), https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf.

36. "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," (Financial Crimes Enforcement Network, May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

37. "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," (Financial Action Task Force, June 21, 2019), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

38. "Explanatory Brief on the Payment Services Bill," (Monetary Authority of Singapore, November 19, 2018), https://www.mas.gov.sg/news/speeches/2018/explanatory-brief-on-the-payment-services-bill.

39. "Overview of Regulatory Sandbox," (Monetary Authority of Singapore), https://www.mas.gov.sg/development/fintech/regulatory-sandbox.

40. The 2020 National Illicit Finance Strategy calls for a reduction in the dollar threshold for the travel rule, which requires the collection of certain identifying information for cross-border transactions. Treasury argues that the $3,000 threshold is too high in a world where virtual currency makes smaller transfers easier. "National Strategy for Combating Terrorist and Other Illicit Financing: 2020," 41.

41. Coats, "Worldwide Threat Assessment of the US Intelligence Community," 16.

42. "Global Trends: Paradox of Progress" (National Intelligence Council, January 2017), 21. https://www.dni.gov/index.php/global-trends-home.

43. Jonathan B. Tucker, "Introduction," in Jonathan B. Tucker, ed., "Double-Edged Innovations: Preventing the Misuse of Emerging Biological/Chemical Technologies," Report No. ASCO 2010 018 (Defense Threat Reduction Agency, 2010), 11, https://apps.dtic.mil/dtic/tr/fulltext/u2/a556984.pdf.

44. The production of dangerous pathogens, for example, requires "an interdisciplinary team of scientists and engineers" who need expertise in a variety of fields to create a pathogen on an industrial scale and deliver it via stable methodology to an adversary in a way that limits accidental disclosure, as Jonathan B. Tucker writes. "States are more likely to be capable of organizing and sustaining such a team than are non-state actors." Jonathan B. Tucker, "Review of the Literature on Dual-Use," in Jonathan B. Tucker, ed., "Double-Edged Innovations: Preventing the Misuse of Emerging Biological/Chemical Technologies," Report No. ASCO 2010 018 (Defense Threat Reduction Agency, 2010).

45. Antonio Regalado, "Top U.S. Intelligence Official Calls Gene Editing a WMD Threat," *MIT Technology Review* (February 9, 2016), https://www.technologyreview.com/s/600774/top-us-intelligence-official-calls-gene-editing-a-wmd-threat/.

46. Jonathan Tucker, "Combinatorial Chemistry and High-Throughput Screening," in Jonathan B. Tucker, ed., "Double-Edged Innovations: Preventing the Misuse of Emerging Biological/Chemical Technologies," Report No. ASCO 2010 018 (Defense Threat Reduction Agency, 2010).

47. Amy E. Smithson, "Chemical Micro Process Devices," in Jonathan B. Tucker, ed., "Double-Edged Innovations: Preventing the Misuse of Emerging Biological/Chemical Technologies," Report No. ASCO 2010 018 (Defense Threat Reduction Agency, 2010).

48. Alexander Kelle, "Synthetic Biology with Standardized Parts," in Jonathan B. Tucker, ed., "Double-Edged Innovations: Preventing the Misuse of Emerging Biological/Chemical Technologies," Report No. ASCO 2010 018 (Defense Threat Reduction Agency, 2010).

49. Gerald Epstein, "DNA Shuffling and Directed Evolution," in Jonathan B. Tucker, ed., "Double-Edged Innovations: Preventing the Misuse of Emerging Biological/Chemical Technologies," Report No. ASCO 2010 018 (Defense Threat Reduction Agency, 2010).

50. Marcel Angliviel de la Beaumelle, Benjamin Spevack, and Devin Thorne, "Open Arms: Evaluating Global Exposure to China's Defense-Industrial Base," (C4ADS, October 2019), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5d95fb48a0bfc672d825e346/1570110297719/Open+Arms.pdf.

51. Elsa Kania and Wilson Vorndick, "Weaponizing Biotech: How China's Military Is Preparing for a 'New Domain of Warfare,'" DefenseOne.com, August 14, 2019, https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/?oref=defense_one_breaking_nl.

52. The Australia Group, for example, is an international coalition of like-minded states that coordinate on dual-use control legislation and regulation.

53. Jonathan B. Tucker, ed., "Double-Edged Innovations: Preventing the Misuse of Emerging Biological/Chemical Technologies," Report No. ASCO 2010 018 (Defense Threat Reduction Agency, 2010), 116.

54. "Destruction of declared Syrian chemical weapons completed," Organisation for the Prohibition of Chemical Weapons, press release, January 4, 2016, https://www.opcw.org/media-centre/news/2016/01/destruction-declared-syrian-chemical-weapons-completed.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

© 2020 Center for a New American Security.

All rights reserved.

1152 15th Street, NW Suite 950 Washington, DC 20005
t. 202.457.9400 | f. 202.457.9401 | info@cnas.org | cnas.org


Center for a
New American
Security