EMERGENT TECHNOLOGY IN THE COMPETITION SPACE: CRYPTORUBLE AND US NATIONAL SECURITY

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Strategic Studies

by

MICA J. HALL, DEPARTMENT OF THE ARMY CIVILIAN
Ph.D., University of Washington, Seattle, Washington, 1997

Fort Leavenworth, Kansas
2020

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED *(From - To)*
12-06-2020	Master's Thesis	AUG 2019 – JUN 2020

4. TITLE AND SUBTITLE

Emergent Technology in the Competition Space: Cryptoruble and US National Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Mica Hall

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In a global environment in which the economic tool of statecraft is as integral to national security as diplomacy, information, and military, Russia's proposed cryptoruble poses a unique threat. Like traditional cryptocurrencies, cryptoruble will used distributed ledger technology; unlike traditional cryptocurrencies, cryptoruble will not be anonymous and emissions will be centrally controlled and likely infinite. The question this thesis answers, "What ramifications does cryptoruble have for US national security?" yields three primary results. After comparing Russia's native cryptocurrency effort to case studies of Venezuela's and Iran's efforts, and looking to Russia's National Security Strategy and news around the launch. Result 1: Russia appears poised to use cryptoruble to circumvent US/Western economic sanctions. If other state or non-state actors accept it as payment, Russia may be able to obtain new energy technologies and/or cyber capabilities, or set up banking/financial institutions outside the US Dollar/SWIFT dominated system. Result 2: After reviewing relevant US strategies and analysis regarding the future of the global order, the US can approach cryptoruble proactively by exploiting its traceability to track currency flows and engage in deterrence in the competition space. Result 3: This thesis identifies a gap between the direction provided by the US National Security Strategy in broad brushstrokes and the more detailed guidance a National Economic Security Strategy could provide by focusing on the nexus of threats to economic and cyber security. If the US intends to respond to threats to its national security in a timely manner, it will still use sanctions as a useful tool, while adding additional cyber and strategy tools to its toolbox.

15. SUBJECT TERMS

Cryptoruble, circumventing sanctions, cryptocurrency, national security, distributed ledger technology

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. PHONE NUMBER *(include area code)*
(U)	(U)	(U)	(U)	125	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Mica Hall

Thesis Title: Emergent Technology in the Competition Space: Cryptoruble and US National Security

Approved by:

_____, Thesis Committee Chair
David A. Anderson, DBA

_____, Member
LTC Romae M. Araud, M.A.

_____, Member
LTC Michael B. Stokes, M.S.

Accepted this 12th day of June 2020 by:

_____, Director, Office of Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

EMERGENT TECHNOLOGY IN THE COMPETITION SPACE: CRYPTORUBLE AND US NATIONAL SECURITY, by Mica Hall, 125 pages.

In a global environment in which the economic tool of statecraft is as integral to national security as diplomacy, information, and military, Russia's proposed cryptoruble poses a unique threat. Like traditional cryptocurrencies, cryptoruble will used distributed ledger technology; unlike traditional cryptocurrencies, cryptoruble will not be anonymous and emissions will be centrally controlled and likely infinite. The question this thesis answers, "What ramifications does cryptoruble have for US national security?" yields three primary results. After comparing Russia's native cryptocurrency effort to case studies of Venezuela's and Iran's efforts, and looking to Russia's National Security Strategy and news around the launch. Result 1: Russia appears poised to use cryptoruble to circumvent US/Western economic sanctions. If other state or non-state actors accept it as payment, Russia may be able to obtain new energy technologies and/or cyber capabilities, or set up banking/financial institutions outside the US Dollar/SWIFT dominated system. Result 2: After reviewing relevant US strategies and analysis regarding the future of the global order, the US can approach cryptoruble proactively by exploiting its traceability to track currency flows and engage in deterrence in the competition space. Result 3: This thesis identifies a gap between the direction provided by the US National Security Strategy in broad brushstrokes and the more detailed guidance a National Economic Security Strategy could provide by focusing on the nexus of threats to economic and cyber security. If the US intends to respond to threats to its national security in a timely manner, it will still use sanctions as a useful tool, while adding additional cyber and strategy tools to its toolbox.

ACKNOWLEDGMENTS

I wish to express my sincere appreciation to my thesis committee Chair, Dr. Dave Anderson, who provided encouragement and support from the beginning and throughout, challenged my ideas to improve my argument, and helped me stay focused. Mr. Tom Wilhelm at the Foreign Military Studies Office served as a sounding board for my topic and a tireless advocate for my efforts. Special thanks to Ms. Jumana Kawar and Ms. Eileen Mehmedali for their instructive and thoughtful feedback on my work. I also wish to acknowledge the support and love of my family and friends, without whose feedback and daily buoying this work would not have been possible.

TABLE OF CONTENTS

Page

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

> In September 2017, at the opening ceremony of a festival in Sochi celebrating the new school year, President Putin told students, "Whoever becomes the leader in AI will become the ruler of the world."
>
> Maksim Oreshkin, Minister of Economic Development, added, "If AI existed, and if it wanted to take over the world and make human beings its slaves, the first thing it would invent would be Bitcoin."
>
> According to the syllogism, Russia intends to control us all.
>
> —.M. Flammini, "The Russian Version of Bitcoin, the Cryptoruble, Has Appeared"

Weaponizing an Economy: The Case of Russia's Cryptoruble

While the investment phenomenon of cryptocurrencies has captured global attention, much less consideration has been paid to the details of their potential as a financial weapon. Cryptocurrencies and the technology on which they are based can have both strategic and tactical level effects. Cryptocurrencies in a weaponized form, and their blockchain or other distributed ledger technology (DLT) bases, can be examined from two perspectives: in the hands of non-state actors and in the hands of state actors. While cryptocurrencies were invented by non-state actors, ostensibly for the purpose of circumventing the banking system and avoiding state-issued currencies, this paper addresses only the use of these tools in the hands of the state, and specifically looks at the Russian case in its initial period of considering the legality of traditional cryptocurrencies and how to harness that technology to its advantage. Russia's decision for how to use DLT applications in the future will become increasingly significant, as "increased competition over international rules will be most apparent in instances where they are poorly defined, such as . . . the use of . . . cyberspace for economic . . . purposes."[1]

Why the "E" in DIME is Growing in Importance

Both cryptocurrencies and DLT have clear implications for the operational environment and present security issues across domains: in addition to the purely economic implications, the development of "traditional" cryptocurrencies, national cryptocurrencies, and national blockchain-type technologies affect domestic infrastructure, the race for information sovereignty, domestic politics, and geopolitics. While state-issued "cryptocurrencies" may appear to be a purely economic endeavor, the state can use its total access to its citizens' personal information to affect social and political change, control information flows, and affect foreign relations both at a regional and world level. More immediately, in the hands of state actors, the ostensibly financial tool of traditional cryptocurrencies, untethered from traditional economic paradigms, can be exploited for their untraceable nature. If money is an idea, based on trust, understanding it is an information-related capability. A country's degree of digital sovereignty can have foreign policy and military consequences, so controlling information is significant in hybrid warfare.

Trends and conditions may intersect, compound, or amplify one another to create complex contexts, and "the impact of the development of so many new and potential[ly] revolutionary technologies is made all the more disruptive by the convergence phenomenon."[2] The cryptoruble demonstrates the national security significance of the intersection of economic tools and technological innovations. The confluence of economic and military factors may also create instability. Using the cryptoruble or mining traditional cryptocurrencies would allow Russia to engage a wide variety of proxy actors to "provide plausible deniability, yet directly allow them to not only shape the

battlespace, but even achieve their objectives without risking a wider conflict. Similarly, they also may choose to work with, sponsor, or support terrorist or criminal entities to achieve a similar end."[3]

Once Russia has established the use of the cryptoruble as an accepted form of payment, the confluence of economy and geopolitics will likely create even more churn. Although the cryptoruble may be tied to the national jurisdiction, Gregory Gleason, professor of Eurasian Security Studies at the George C. Marshall European Center for Security Studies, places it squarely in "the competition among the national currencies and even consideration of the adoption of alternative currencies… reflecting geopolitical rivalry rather than conventional monetary policy."[4] This newfound economic might could put the teeth into the coercive diplomacy Russia would use to otherwise get the former Central Asian republics to participate in trade deals based on a non-USD reference currency and/or participate in banking activities that avoid the SWIFT system of interbank money transfers. By 2035-2050, "great powers [will] have converted hybrid combinations of economic power, technological prowess, and virulent, cyber-ideologies into effective strategic strength…to assert or dispute regional alternatives to established global norms."[5]

In Dmitry Lebedev's view, "The focus on technological and digital sovereignty in an era of communication that is challenging traditional political geographies is a crucial feature of the modern Russian state."[6] While cryptocurrencies created by non-state actors may be a questionable personal investment, we have only begun to see how DLT-based currency and applications can evolve in the hands of a nation-state, and how Russia will use them in the name of national security.

Despite a short respite of closer ties and cooperation with other countries across the globe, the US future now seems more likely to hold "challenges from both persistent disorder and states contesting international norms,"[7] particularly Russia and China, which the 2017 US National Security Strategy (NSS) describes as "attempting to erode American security and prosperity . . . [and] make economies less free and less fair."[8] In determining the sources of disruption, analysts can look across the DIME spectrum, especially as "China, Russia, and other countries now routinely look to geo-economics as a means of first resort, often to undermine U.S. power and influence."[9] While "strategic studies is often narrowly interpreted as the study of military power . . . it is not its totality," and the cryptoruble strategy merits a geo-economic approach, namely, "exploring how economic tools are sharpened for great power competition."[10] Cryptoruble is a geo-economic tool in Russia's great power competition toolbox, so while the US endeavors to use economic tools such as sanctions, "the United States has a genuine geopolitical interest in keeping shows of economic coercion to a minimum."[11] Whether characterized as coercion or persuasion, since 2014 sanctions have had only limited success in changing Russian behavior. Strategists need to consider new tools[12] to execute on NSS imperatives to put economic pressure on security threats and sever their sources of funding.[13]

Emergent and Disruptive Technologies

Cyberspace has opened up another domain in which Russia competes with the US and in which the US exercises its elements of national power,[14] and the implications of "central bank digital currencies" like cryptoruble "for international sanctions are vast."[15] In October, 2017, Russia officially stated it would create a national cryptocurrency, the

cryptoruble. Cryptocurrency experts have already determined the "crypto" prefix of cryptoruble to be a misnomer, insofar as it will not be anonymous, as "traditional" cryptocurrencies are. Unlike the current version of digital currencies, which are already used for electronic funds transfers, the cryptoruble will use a distributed ledger technology (DLT). It may be of the blockchain variety, such as that used by Bitcoin, or it may be of the snowball variety or some other branching shape. Like traditional cryptocurrencies, cryptoruble transactions will take place via decentralized solution of encryption math problems, but the transactions will not be anonymous and ownership will be identifiable. This traceability has significant implications for cryptoruble, which is intended to allow the government to track transactions, senders, and receivers. To deter Russia from circumventing sanctions, the US could take advantage of the cryptoruble's traceability and build the capacity to trace cryptoruble flows.

Emergent technologies such as cryptoruble "are changing both the character and prospects of conflict," specifically, "the ability of states to mount and sustain conflict".[16] along the along the cooperation-conflict continuum. It its search for proactive approaches to countering the cryptoruble and protect itself and its security interests, the US could establish a National Economic Security Strategy (NESS) to address national security issues at the nexus of economics and cybersecurity. The NESS would flesh out guidance from the NSS to government organizations, especially in the Intelligence Community (IC), to support creating and implementing protective economic measures in cyberspace.

As RAND authors James Dobbins et al. noted in their review of cost-imposing options to change Russian behavior, "The maxim that 'Russia is never so strong nor so weak as it appears' remains as true in the current century as it was in the 19th and

20th."[17] In the split-screen reality that is the current Russian media-scape, the cryptoruble is billed as part of the digital economy that will help the country escape the US Dollar (USD)-domination of the world economy and establish digital sovereignty. According to journalist Kyree Leary, "Digital currencies and tokens are expected to influence the creation of a new digital economy, but predicting the future of crypto in Russia once these new regulations are in place is impossible."[18] The state appears to be pursuing both control of information flow inside the country, as well as an outward stance that is part isolationist, part regional hegemon.

Time will tell how Russia's plans for a national cryptocurrency will affect its position in the world and its ability to exert power nationally, regionally, and worldwide. Based on the wide variety of statements coming from Russian state sources, Russian experts, and Russian citizens, the nation has caught the cryptocurrency fever. Russian officials have already painted a picture of the key elements of cryptocurrency for the country, and the Russian-language Internet has discussed in depth the national security, economic, and data protection creating a new digital currency will have. Although Russia has only engaged in experiments so far, they have had far-reaching significance in that they represent what the state can do with true information sovereignty. With geopolitics a consistent motivation for Russia[19] and government sources repeatedly emphasizing that the Digital Economy as not only an economic program, but a matter of national security, the implications for the rest of the world are apparent: between the cryptoruble and state mining of traditional cryptocurrencies, distributed ledger technology provides a new financial weapon for a new generation of conflict.

This thesis seeks to answer the question: What are the ramifications of a Russian cryptoruble for US national security? The analysis focuses on Russia's approach to Western sanctions against it, the features of cryptoruble as a financial instrument, and cybertools, and the US assessment of and approach to Russia as a national security threat. Once the potential threats from cryptoruble are determined, this analysis will recommend appropriate responses, based on official US national security goals and capabilities.

---

[1] U.S. Joint Chiefs of Staff (JCS), *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (JOE 2035) (Washington, DC: Department of Defense, July 14, 2016), http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.

[2] U.S. Army Training and Doctrine Command (TRADOC) G-2, *The Operational Environment and the Changing Character of Future Warfare* (Fort Eustis, VA: TRADOC, 2017), https://community.apan.org/wg/tradoc-g2/mad-scientist/m/visualizing-multi-domain-battle-2030-2050/200203.

[3] JCS, JOE 2035.

[4] Gregory Gleason, "Currency Wars along the Silk Road. Which will emerge on top in Central Asia: The dollar, the yuan, or even Bitcoin?" *The Diplomat*, July 27, 2017, http://thediplomat.com/ 2017/07/currency-wars-along-the-silk-road/.

[5] TRADOC, *The Operational Environment and the Changing Character of Future Warfare*.

[6] Dmitriy Lebedev, "Digital Sovereignty à la Russe," Open Democracy, November 3, 2017, https://www.opendemocracy.net/od-russia/dmitry-lebedev/digital-sovereignty-a-la-russe.

[7] U.S. Army Training and Doctrine Command (TRADOC), TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 2018), 6.

[8] U.S. President, *National Security Strategy of the United States of America* (NSS) (Washington, DC: The White House, December 2017), 2.

[9] Robert D. Blackwill and Jennifer M. Harris, "The Lost Art of Economic Statecraft: Restoring an American Tradition," *Foreign Affairs* (March/April 2016), https://www.foreignaffairs.com/articles/2016-02-16/lost-art-economic-statecraft?cid=nlc-fatoday-20160226&sp_mid=50791614&sp_rid=bWFyay5yLndpbGNveC5jaXZ

AbWFpbC5taWwS1&spMailingID=50791614&spUserID=NTI0MzQxODE4NDIS1&spJobID=863297564&spReportId=ODYzMjk3NTY0S0.

[10] IISS, "War, power, rules, accessed December 12, 2019, https://www.iiss.org/research/war-power-rules.

[11] Blackwell and Harris, "The Lost Art."

[12] Ibid.

[13] U.S. President, NSS, 34.

[14] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, no. 73 (2nd Quarter 2014): 13.

[15] Tanvi Ratna, "Iran Has a Bitcoin Strategy to Beat Trump," *Foreign Policy*, January 24, 2020, https://foreignpolicy.com/2020/01/24/iran-bitcoin-strategy-cryptocurrency-blockchain-sanctions/.

[16] IISS, "War, Power, Rules."

[17] James Dobbins, Raphael S. Cohen, Nathan Chandler, Bryan Frederick, Edward Geist, Paul DeLuca, Forrest E. Morgan, Howard J. Shatz, and Brent Williams, *Overextending and Unbalancing Russia: Assessing the Impact of Cost-Imposing Options* (Santa Monica, CA: RAND Corporation, 2019), 2. https://www.rand.org/pubs/research_briefs/RB10014.html.

[18] Kyree Leary, "Vladimir Putin Just Revealed Russia's Plans for Cryptocurrencies," *Futurism*, October 26, 2017, https://futurism.com/vladimir-putin-just-revealed-russias-plans-for-cryptocurrencies/.

[19] Madhvi Mavadiya, "Putin and Ethereum: A Match Made In Fintech," *Forbes*, August 29, 2017, https:// www.forbes.com/sites/madhvimavadiya/2017/08/29/putin-ethereum-fintech/ #76e2a6f16b5c.

CHAPTER 2

LITERATURE REVIEW

When President Putin announced the launch of the cryptoruble in October 2017, Russian officials, analysts, and netizens, and US and European analysts reacted with surprising consensus that Russia would likely try to use it to circumvent Western economic/trade sanctions. The Russian government could use cryptoruble to alleviate the effects of several sanctions by (1) finding a trading partner from whom to purchase energy-sector technologies and financial services it is currently being denied; (2) creating its own banking and money transfer system with cryptoruble as the common reference currency; (3) a combination of both.

The Official Russian View

According to Financial *Times* and *Pravda*, Kremlin insiders have suggested the cryptoruble could be "a useful means of avoiding sanctions against Russia and neighboring countries" and "may help the country avoid Western sanctions."[1] Presidential Economic Advisor Sergey Glazyev offered sanctions evasion as the basis of the "objective need" for the cryptoruble.[2] As he reasons, "Banks are subject to sanctions, as we know, and don't want to settle accounts. This instrument is a good fit for activities that are sensitive for the government. Despite the sanctions, we can settle accounts with our counterparts around the world,"[3] specifically, "with no regard for sanctions."[4]

As a parallel system to normal economic trade, the cryptoruble could both circumvent sanctions by "building a new system of transfers in exchange for the delivery of strategically important goods," while serving as a "unique format for investing in

Russian companies."[5] According to the plan President Putin laid out upon announcing the launch of cryptoruble, Russia would take advantage of its dominant member status in the Eurasian Economic Union (EAEU) to establish a "single payment space" for the member states of the EAEU, with ready-made trading partners, based on "the use of new financial technologies, including the technology of distributed registries."[6] Glazyev's suggestion is that a cryptoruble would only be used as an alternative to the ruble or other payments as needed. According to the pro-cryptoruble economist, it would be used, "only for those things for which it's designated, only in the legal field allowed. . .Wherever there's a need for a targeted use of money, be it government expenses, budget investments, or the work of banks and corporations, it can be used."[7]

Russian leadership may experiment with the cryptoruble using Crimea as its Petri dish. To that end, Russian politicians have suggested establishing a foreign policy "sandbox" to determine if a domestic cryptocurrency could be used as an end run around international sanctions. As Russian politician and Presidential Commissioner for Entrepreneurs' Rights Boris Titov envisions it, this "Black Sea-licon Valley" would serve as a testbed for developing domestic DLT systems and could attract much needed outside investments into the Russian economy.[8] According to Titov, if other countries are willing to accept a domestic cryptocurrency as payment, it could replace the outdated SWIFT bank transfer system.[9] As reported in *Svobodnaya Pressa*, "The idea of turning Crimea into a full-blown blockchain zone is being discussed at all levels, from MinFin to the President's administration. The belief is that Crimea, thanks to its special status in the world, even given the sanctions, could show how blockchain and its decentralization

would allow for building a new form of business,"[10] thus facilitating economic deals outside the scope of hard-currency-based sanctions.

Russian Analysis

Russian financial analyst Fyodor Naumov argues the government should create a national cryptocurrency and do so quickly, particularly given recent sanctions and the threat of additional sanctions by the US and EU.[11] In his detailed response to the announcement of the cryptoruble launch, "Why The Government Needs The Cryptoruble," Naumov points out, these sanctions have highlighted Russia's high level of global interdependence and dependence on "Western technologies," as well as the likelihood that Russia will lose even more access to global financial markets or lose it completely. He makes the economic argument: "It is hard to imagine how the Russian economy would operate. It is clear Russia would be abandoned to the technology of several decades ago. There are tech workarounds, like the Mir payment system, but they would take too long and would be too expensive to go back to."[12]

As Naumov suggests, Russia could mitigate sanctions effects by extracting itself from the international banking system: The value of a cryptocurrency's anonymity could significantly help the "de-dollarization" effort, while also serving as a preventative strike by "allow[ing] for greater security of international payments and allow[ing] [Russia] to stop using the SWIFT system, which Russia could be shut out of anyway, as part of another round of sanctions."[13] For Naumov, the cryptoruble provides a means of national security and self-preservation: "The introduction of sanctions has shown that Russia must create its own systems and its own technologies, in order to not find itself cut off from the global technology infrastructure."[14]

Several other blockchain experts also characterize the cryptoruble effort as a way out of the USD-dominated international financial system. As blockchain expert Evgeniy Glariantov suggests, a cryptoruble could help unseat other digital payment systems like Visa.[15] Tech journalist, editor, and self-styled hacker "alizar" calls cryptoruble a significant step away from a USD-pegged economy, and says introducing national cryptocurrencies in multiple countries could hasten such a dethroning.[16]

US Analysis

Eurasia expert Gregory Gleason believes the Russian administration took an "if you can't beat 'em, join 'em" approach to cryptocurrency when it recognized this cyber-technology was a "juggernaut that could not be simply ignored or dismissed."[17] Russia had already shown a desire to find a way to execute financial transactions beyond its borders using something other than USD. According Gleason, in 2014, China and Russia signed a number of currency swap agreements, "designed to habituate making authorized bilateral financial transactions without denomination in USD."[18] In 2015, the two countries signed an agreement to peg/re-peg their national currencies to the value of gold, and, according to Gleason after the International Monetary Fund included the RMB in its Special Drawing Rights, "Russian authorities began to promote the idea of a gold-based cryptocurrency, managed by China or Russia,"[19] to pull China towards itself and away from the international system. While ignoring the severe risk of secondary sanctions for China, the idea of a new, shared gold-based digital currency is "one of the most discussed policy innovations" in the conservative Eurasianist political-ideological movement, which has supporters in the current administration.[20] Gleason concludes the decision to

launch cryptoruble is more politically than economically motivated,[21] and cryptoruble will be used to political ends.

Ray Finch, Kansas University Center for Russian, East European, and Eurasian Studies, concludes in his 2015 analysis of the Kremlin's approach to the Russian economy, that Russia "appears increasingly willing to go further in playing economic hardball," and that unseating the USD would allow for a preferred, multipolar world to emerge,[22] appears to hold true today. Russia has started by cleaning its own house, decreasing its own "dollar-denominated assets held by its central bank," passing laws designed to "limit its citizens from holding foreign property or foreign bank accounts," and "campaigning for oligarchs to repatriate their assets back to Russia and exchange them for rubles."[23]

President Putin's campaign to unseat the USD stems from his desire to regain geopolitical power in the world. As Finch suggests, "The Kremlin leadership . . . see[s] a direct nexus between dominant U.S. military power and the status of the dollar as the global reserve currency."[24] He goes on to say, "the Kremlin reasons that replacing the USD as the global reference currency would force the US to reduce spending overall, including on its military, which would open the door for Russia to regain at least regional dominance and "maintain its legitimate sphere of interest."[25] According to this logic, a multipolar system would replace the US hegemony and would be "inherently more stable, as each major power will be more inclined to maintain a peaceful balance of power."[26] A Sino-Russian pole would cover "a large, resource-rich swath of Eurasian and Asian land . . . complete with its own institutions, markets, security infrastructure, currency, and payment mechanisms, bypassing the dollar-based system if necessary."[27]

Whether Russian leaders use cryptoruble to make surreptitious purchases to fly under sanctions radar or to openly establish their own trading system and thumb their nose at the international financial system, crypto technologies will likely facilitate the process. Analyst Jake Frankenfield suggests one of President Putin's primary interests in cryptoruble is that its transactions are encrypted "and thus easier to discreetly send money without worrying about sanctions placed on the country by the international community."[28] As former FBI agent Mark Johnson has suggested, the Kremlin will be able to get around financial sector sanctions and carry out financial operations in cryptorubles,[29] and will subsequently attract financing back to Russia.[30]

Effectiveness of Sanctions Against Russia

A review of current US and EU sanctions against RU reveals the mixed effectiveness of current sanctions, however, the literature shows agreement that both in general and in the case of US and EU sanctions against Russia, economic sanctions are more effective in conjunction with other factors contributing to a bad economy, i.e. economic sanctions make a bad economy worse. In 2016, President Putin acknowledged the effects of sanctions on the Russian economy, stating, "It's obvious that external limitations have reduced our access to financial resources for companies and individuals . . . Overall, economic financing is unstable."[31]

In 2019 the Congressional Research Service (CRS) reviewed the effects of US sanctions against Russia on its economy overall and found their effectiveness fluctuated with oil prices. As Cory Welt et al. of CRS suggest, "It is difficult to disentangle the impact of sanctions imposed on Russia, particularly those related to its invasion of Ukraine, from fluctuations in the global price of oil, a major export and source of revenue

for the Russian government."[32] This is even more important in an economy that is so vulnerable because it is lacks diversification. Sectoral sanctions on both finance and energy technologies added pressure, but "the 2014 collapse in global oil prices had a larger impact than sanctions,"[33] and when oil prices rose in 2016-2017, Russia's economy improved,"[34] so sanctions alone are not enough to keep the economy depressed. In addition, the Obama Administration and EU Ukraine-related sanctions were specifically crafted to have a low impact on the economy over all, rather they were intended to "target individuals and entities responsible for offending policies and/or associated with key Russian policymakers in a way that would get Russia to change its behavior while minimizing collateral damage to the Russian people."[35] And even those targeted sanctions are Western leaders must face the uncomfortable fact that for now sanctions are "failing to shake Vladimir Putin's position in the Kremlin,"[36] which means no change in behavior.

While "oil prices, not sanctions, drove changes in the value of the ruble,"[37] sanctions combined with the other "hammer blows" of falling oil prices and a collapsing currency, to drive Russia's stagnating economy into decline.[38] Ian Bond et al., at the Center for European Reform, draw the thread out further, indicating that lower oil revenues start the cycle by affecting the ruble, which fuels a "loss of confidence in the Russian economy," which, combined with "financial sanctions and political uncertainty . . . [leads] to capital flight as wealthy Russians and foreign investors dump ruble assets . . . [which leads] to a collapse in investment, which further weakens the economy, but also exacerbate[es] the fall in the currency."[39] Recent downturns in the Russian economy caused by the combination of previous sanctions and lower in oil prices have led analysts

to predict Russia will pursue a solution by controlling something they can, namely, bypassing sanctions. Given the concentration of national statecraft tools in one place, these political-economic problems are pushing Russia "down the path of political economic isolation," which is forcing the leadership to "find new outlets for the Russian economy."[40]

While Russian leaders may have grown accustomed the additional weight of current financial sanctions on the economy, one sanction the economy would not survive without a safety net or backup plan is being excluded from the SWIFT international bank transfer system. Herman Gref, head of the government savings bank Sberbank, has suggested such a move would be catastrophic for Russia, saying, "The Cold War would look like child's play compared to the new US sanctions that could be introduced at the beginning of 2018,"[41] when the idea 2014 threat came up again in 2017. According to Bond et al., SWIFT "has a de facto monopoly on simple and secure international money transfers. The knock-on effects on Russia's financial system and international trade are potentially large, especially in the short run when no alternatives exist."[42] Russia does have its own internal transfer system, MIR, but they would need international buy-in for it to help the Russian economy. And while there has been no indication US leadership would activate this "nuclear option", the threat does appear to serve as yet another motivation to create a USD bypass.

The literature from US, European, and Russian sources shows broad agreement that sanctions do have some effect. Sanctions are necessary but not sufficient, so the US is likely to keep sanctions in place to keep the pressure on, and is likely to care if Russia tries to circumvent those sanctions. The answer to the question as to what other tools the

US can fruitfully use in conjunction with sanctions to achieve its desired objectives may lay in the cryptoruble, the very tool Russia appears poised to use to circumvent those sanctions ill effects.

US Assessment of The Russian Threat

Review of US national security policy indicates the US regards Russia as a (near-) peer adversary who is actively working against US national interests, and underscores US commitment to finding ways – including but not limited to sanctions – to deter and defeat any actions malign actors, including Russia, take against US national security. The US National Security Strategy, National Cyber Strategy, and National Intelligence Strategy all name Russia explicitly as a threat to US national security, particularly in the competition space below the threshold of armed conflict. While Russia and China are often cited in tandem as (near-)peer threats or as the pacing threat and emerging threat, respectively, the assessment of their weaknesses diverges, and a unique picture emerges for how to approach Russia's critical vulnerabilities and center of gravity.

Russia's center of gravity is the Russian leadership itself, specifically, Putin's inner circle, "what has been called Putin's 'vertical of impunity,'" often simply referred to as 'the vertical'.[43] According to Howard Dobbins of the RAND Corporation, "The Russian leadership's greatest anxiety concerns the stability and durability of the regime."[44] Dobbins, a former Assistant Secretary of State for Europe, and his RAND colleagues, call "Russia's greatest vulnerability its economy," namely because it lacks diversification and it relatively small compared to other 'great powers'.[45] The vertical's primary critical capability is its ability to make money nominally for government coffers, but factually for themselves. According to Karen Dawisha, a kleptocracy scholar, "Putin

has built a legalistic system, but its net effect is to control, channel, and coerce the middle class and the broader elite while at the same time allowing the inner core to act in accord with according to the adage "For my friends, anything. For my enemies, the law!"[46]

As Dobbins et al. suggest in their comprehensive 2019 report, "Overextending and Unbalancing Russia: Assessing the Impact of Cost-Imposing Options," the most effective approach the US can take to protecting its national security from the Russian threat is to "extend Russia" by "directly address[ing] its vulnerabilities, anxieties, and strengths, exploiting areas of weakness while undermining Russia's current advantages."[47] In Putin's version of state capitalism – not so much centralized production as a centralized bank account – which Dawisha characterizes as "a system based on massive predation on a level not seen in Russia since the czars," state-owned enterprises and state-owned banks with oligarch directors combines the worst of both Communism and capitalism, "the state nationalizes the risk but privatizes the rewards to those closest to the president in return for their loyalty."[48] The US continues to treat Putin as a legitimate head of state, while acknowledging its revisionist approach and suggesting it will likely increasingly partner with China to "reorder international rules in their favor."[49]

Russian leaders counter their *anxiety* about their own staying power by directing the society's attention to the threat from without, so approaches to the Russian CoG will take these ideas into account. The Russian National Security Strategy (2014-2016) "highlight[s] Russia's vision of world politics as struggle for resources and power, as well as a heightened sense of danger toward Russia."[50] According to leading post-Soviet Eurasianists and as espoused by President Putin, leaders "belie[ve] in the pre-eminence of

the ‘sacred’ state over the individual, in the special mission of the Russian people in the modern world, and in the *vulnerability* of Russian sovereignty to the encroachments of a hostile West.”[51]

Meanwhile, Treasury has already identified Russian efforts to evade US sanctions and has taken the “name and shame” approach to “ensure that the public is aware of the tactics undertaken by designated parties and [ensure] that these actors remain blocked from the U.S. financial system” using the Countering America’s Adversaries Through Sanctions Act (CAATSA).[52] Russia’s *strength* in these efforts will likely come from its integrated statecraft efforts including “a range of cyber activities [which] will be increasingly and more comprehensively linked with national security strategies,”[53] even if they are carried out by the central bank instead of by the military.

Gap identified: The analysis published about this topic addresses various aspects around the periphery and sets the environment to answer the research question, and this thesis examines recent events, motivations of key actors, and current national security policy, to establish a trend line for future action.

---

[1] “FT: Russia Is Looking For A Way to ‘Cut Off’ Cryptocurrencies,” *Russian RT,* January 2, 2018, https://russian.rt.com/inotv/2018-01-02/FT-Rossiya-ishhet-sposob-ukrotit.

[2] “Sergey Glazyev Explains How a Cryptocurrency Will Help Russia Get around Sanctions,” Smart-Lab, December 13, 2017, https://smart-lab.ru/tag.

[3] “An Unusual Way of Getting around Sanctions Has Been Named,” *Pravda,* December 12, 2017, https://www. pravda.ru/news/economics/12-12-2017/1360371-crypto-0/.

[4] “FT: Russia Is Looking For A Way.”

[5] “Cryptoruble: What Is It And What Will It Be Like?” Altcoin.info, October 16, 2017, https://altcoin.info/news/kriptoruble-chot-eto-takoe-i-kakim-on-budet-872.html.

[6] Leary, "Vladimir Putin Just Revealed."

[7] "Cryptoruble to Save Russia."

[8] Vera Sokolova, "Crypto Way around Anti-Russian Sanctions: Crimea May Become the First Official Blockchain Zone in the World," *Svpressa* (blog), September 1, 2017, http://svpressa.ru/blogs/article/180575.

[9] Ibid.

[10] Ibid.

[11] Fyodor Naumov, "Digital Sovereignty: Why The Government Needs The Cryptoruble," *Forbes*, November 3, 2017, http://www.forbes.ru/finansy-i-investicii/352381-cifrovoy-suvernitet-zachem-pravitelstvu-ponadobitsya-kriptorubl.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] A. Koroleva, "The cryptoruble will be a blow to the existing payment system," Expert Online, October 17, 2017, http://expert.ru/2017/10/17/kriptoruble-udarit-po-platezhnyim-sistemam/.

[16] Alizar, "Putin has Ordered a Russian Cryptocurrency be Issued: The Cryptoruble," *Geek Times,* October 15, 2017, https://geektimes.ru/post/294373.

[17] Gregory Gleason, "FSB Seeks to Forge 'Digital Sovereignty' in Russia's Financial Sector," *Eurasia Daily Monitor*, 14, no. 109, https://jamestown.org/program/fsb-seeks-to-forge-digital-sovereignty-in-russias-financial-sector/.

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] Gleason, "Currency Wars Along the Silk Road."

[22] Raymond Finch, "The Kremlin's Economic Checkmate Maneuver," *Problems of Post-Communism*, 62 (2015): 188.

[23] Ibid., 189.

[24] Ibid., 188.

[25] Ibid.

[26] Ibid.

[27] Enrico Cau, "The Geopolitics of the Beijing-Moscow Consensus," *The Diplomat,* January 4, 2018, https://thediplomat.com/2018/01/the-geopolitics-of-the-beijing-moscow-consensus/.

[28] Jake Frankenfield, "CryptoRuble," Investopedia, June 25, 2019, https://www.investopedia.com/terms/c/cryptoruble.asp.

[29] Sokolova, "Crypto Way Around."

[30] "Putin Has Thought Up A Clever Way to Get around Sanctions; Alarms Are Ringing In The West," Obozrevatel.com, January 3, 2018, https://www.obozrevatel.com/economics/business-and-finance/putin-pridumal-hitryij-sposob-obojti-sanktsii-na-zapade-zabili-trevogu.

[31] President of Russia, "President's Address to the Federal Assembly," Moscow, Kremlin, December 1, 2016, http://kremlin.ru/events/president/transcripts/messages/53379.

[32] Cory Welt, Kristin Archick, Rebecca M. Nelson, and Dianne E. Rennack, *U.S. Sanctions on Russia,* Congressional Research Service Report for Congress R45415 (Washington, DC: Library of Congress, January 11, 2019), 4, https://crsreports.congress.gov.

[33] Ibid., 3.

[34] Ibid., 2.

[35] Ibid., 3.

[36] Ian Bond, Christian Odendahl, and Jennifer Rankin, *Frozen: The Politics and Economics of Sanctions against Russia,* Policy Brief (London, UK: Center for European Reform, March 2015), 11.

[37] Ibid., 44.

[38] Ibid., 6.

[39] Ibid., 7.

[40] Cau, "The Geopolitics."

[41] Max Seddon, "Russian Banker Warns Against New US Sanctions," *Financial Times,* December 24, 2017, https://www.ft.com/content/9c25c852-e400-11e7-97e2-916d4fbac0da.

[42] Bond et al., "Frozen," 10.

[43] Karen Dawisha, "The Putin Principle: How It Came to Rule Russia," *World Affairs Journal* (May/June 2015): 3.

[44] James Dobbins, "Nonviolent Ways the United States Could Exploit Russian Vulnerabilities," The RAND Corporation, April 24, 2019, https://www.rand.org/news/press/2019/04/24.html.

[45] Ibid.

[46] Dawisha, "The Putin Principle," 3.

[47] Dobbins et al., "Overextending and Unbalancing Russia," 12.

[48] Dawisha, "The Putin Principle," 1.

[49] JCS, JOE 2035.

[50] Katri Pynnöniemi, "Russia's National Security Strategy: Analysis of Conceptual Evolution," *The Journal of Slavic Military Studies*, 31, no. 2, (2018): 240 https://www.tandfonline.com/doi/full/10.1080/13518046.2018.1451091? scroll= top& needAccess=true.

[51] Nadezhda Arbatova, "Three Faces of Russia's Neo-Eurasianism," International Institute for Strategic Studies, December 2019-January 2020. https://www.iiss.org/publications/survival/2019/survival-global-politics-and-strategy-december-2019january-2020/616-02-arbatova.

[52] U.S. Department of Treasury, "Treasury Targets Attempted Circumvention of Sanctions," Press Release, August 21, 2018, https://home.treasury.gov/news/press-releases/sm462.

[53] JCS, JOE 2035; Arbatoya, "Three Faces of Russia's Neo-Eurasianism."

CHAPTER 3

RESEARCH METHODOLOGY

Research Question: What are the ramifications of a Russian cryptoruble for US national security?

Limitations: The situation is fluid; facts may change before or after thesis is complete.

Delimitation: Regarding cryptoruble, focus is on October 2017 – December 2019; regarding US and EU sanctions against Russia, 2012 – 2019.

This thesis uses a mixed methodology to answer the research question: What are the ramifications of a Russian cryptoruble for US national security? There are two sources of relevant data: first is a comparative case study of Venezuela and Iran, which are similar in profile to Russia, and who have already launched native cryptocurrencies. Their motivation for establishing their own cryptocurrencies, and the effects those cryptocurrencies have had on US national security provide insight into the operating environment in which Russia is operating as it prepares to launch cryptoruble. An analysis using Mill's method of agreement shows that Russia shares several significant political and economic characteristics with Venezuela and Iran. There is one significant difference that warrants examining data from an additional source: among the three countries, only Russia can be considered a near-peer adversary to the US. As a result, drawing conclusions regarding implications for US national security based on parallels with Venezuela and Iran will likely be based on a partial yet incomplete picture.

The second useful source of data is the most recent National Security Strategy of the Russian Federation. While the international situation has continued to develop and

change since it was published in 2015, it does indicate the direction Russia sees for itself, the goals it plans to pursue for its economic security, including how it views the US and plans for working with the US. It also indicates Russia's goals for restoring its status as a world power, establishing a multipolar world (as opposed to the previous bipolar two-superpower world order), and it points to what it perceives is hurting the Russian economy and what it needs to do to address those problems. No official document states Russia's intent for creating cryptoruble specifically vis-à-vis the US, rather, the President has stated the goals for cryptoruble to be clustered around domestic financial security and, notably, digital sovereignty. Even the statements made by government and banking officials regarding the usefulness of cryptoruble in Russia extricating itself out from under the domination of the USD have their basis in the RU NSS.

Comparative Case Study

As detailed in Rose Mahdavieh's comprehensive review of the factors that lead countries to launch their own cryptocurrencies, Venezuela, Iran, and Russia share several important characteristics: They are led by kleptocratic regimes and their economies are "resource-cursed,"[1] meaning they are not diversified and the overwhelming revenue driver for each is the export of natural resources, namely oil or oil and gas. The combination of these two points is key: the dependence on only energy exports makes the economy subject to the whims of the global market, leading to volatility, and the widespread corruption at the top leads to financial mismanagement and high inflation (Russia) or hyperinflation (Venezuela and Iran). As more producers have entered the energy sector, the price of oil has fallen dramatically and these countries' economies have steadily devolved. The singular plank in their economic platforms have made sectoral

sanctions the US tool of choice to respond to illicit behavior: Iran for sponsoring terrorism, Venezuela for sponsoring narcotrafficking, and Russia for invading a sovereign country (Ukraine) and meddling in US elections, among sanctions for other infractions. These sanctions made the bad economic situation in these countries worse.

In the 2018 Transparency International Corruption Perception Index, least to most, out of 180 countries, Russia ranks 135th, Iran 138th, and Venezuela 168th.[2] Mahdavieh squarely places the motivation for establishing a native cryptocurrency in all three countries as the kleptocracies' desire to strengthen their own position.[3] She identifies the pervasive narrative of fighting against the hegemony of the USD and dependency on the SWIFT system by circumventing US and Western sanctions and establishing their own financial and trade opportunities.[4] Of note, traditional cryptocurrencies were already "in circulation" in these countries before they announced they would launch their own, and citizens of those countries were already habituating, to some degree, to using and especially mining Bitcoin and other cryptocurrencies.[5]

Using Mill's method of agreement, all the aforementioned shared features are *attributes* and are the independent variables in the study. The dependent variable is an *outcome*, and if several attributes are common across multiple cases and the cases end up with the same outcome, it implies a possible correlation, even if it does not show causation. So far, the only threat the Petro and Cryptorial have posed to US national security is still a potential – the possibility of making purchases contravening sanctions. The US stifled those efforts early in the process proposing sanctions against persons or entities trading in those cryptocurrencies.[6] Once Russia launches cryptoruble, the US is likely to propose similar sanctions for anyone using it, however, there is one important

difference between cryptoruble and the other two cryptocurrencies that will likely affect the outcome: there has been no suggestion it will be traded in traditional cryptomarkets, and no indication it will be backed with specific oil, gas, or other resources. Russia's cryptocurrency, rather, will be issued as a central bank digital currency, intended to serve as the sole national currency, not a supplemental financial asset for the government and investors to experiment with. It is not intended to raise money on its own, although in late 2017, the government announced its intent to tax cryptoruble mining and sales (if sold for a profit in exchange for other currency).[7] The consensus among supporters and detractors is that cryptoruble mining and emission will be controlled exclusively by the government. As one FAQ-type article suggests cryptoruble would be traded on traditional currency markets, allowing for exchange between Russian (crypto)currency, traditional cryptocurrencies, and hard currencies. According to the site, "there will be zero anonymity of transactions, but you don't need it in this case, because the goals for this currency are completely different,"[8] indicating the intent is not to market cryptoruble as a traditional cryptocurrency, because it lacks the features that attract buyers, namely, anonymity and decoupling from central banks. In addition to cryptoruble's domestic use, however, it could be used to open trade channels not currently open now due to sanctions.

There is one more significant difference between the Russia case and the other two: the US considers Russia, along with China, as (near-)peer adversaries and thus any innovations in their currency system, especially an instrument that operates in the cybersphere, merits attention. In this respect, China and Russia differ greatly from each other: China's economy is bigger, more diversified, and more globally connected than Russia's. In addition, China has only committed to studying digital currencies and

whether it would be worthwhile to launch their own.[9] Interestingly, widespread mining of traditional cryptocurrencies in China[10] does show something in common with the other cases, namely, something less than a complete rejection of cryptocurrencies and their right to exist in the world as some form of digital asset.[11] This perspective may come into play in future use of cryptocurrencies, either traditional or native.

Figure 1 (below) shows the shared features of countries examined for this thesis regarding their motivations for and efforts in developing native cryptocurrencies.

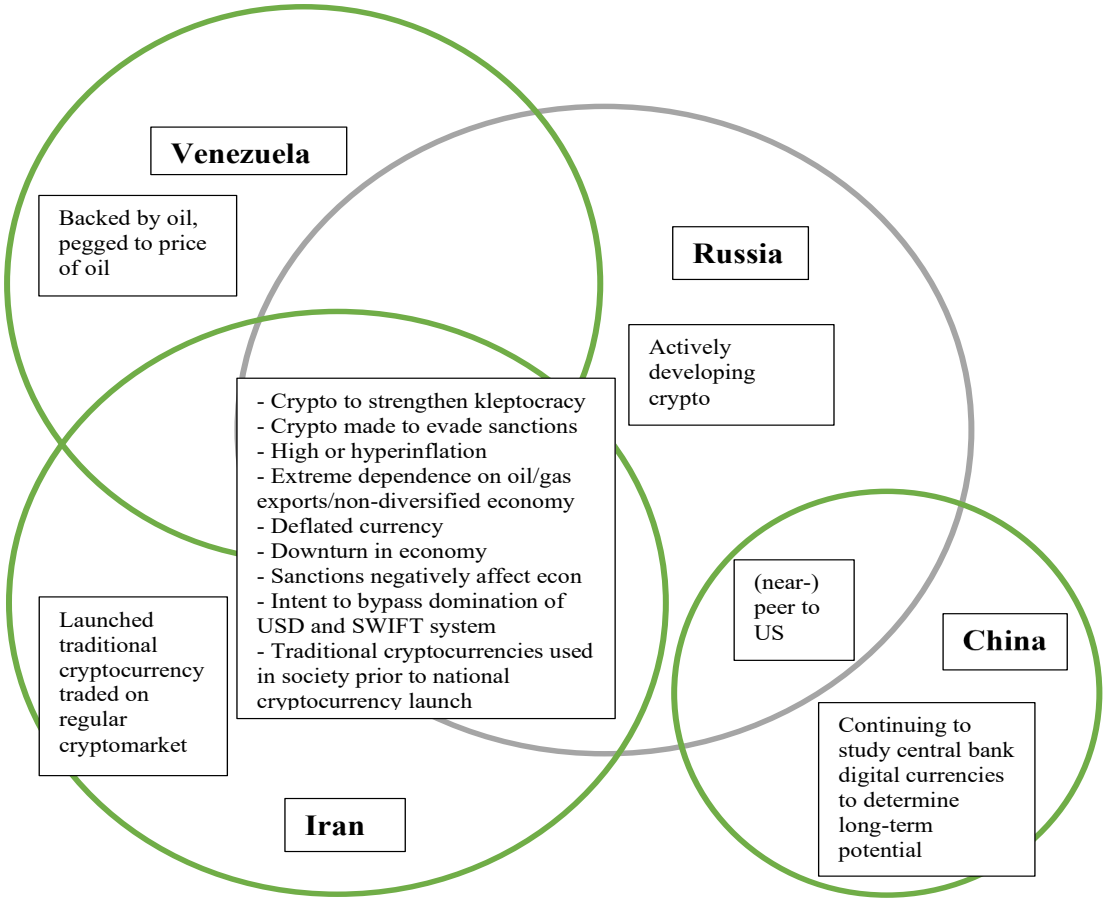

Figure 1. Comparative Case Study: Shared Attributes

Source: Created by author.

National Security Strategy of the RF Until 2020

The comparative case study sheds some light on likely next steps for cryptoruble, particularly how it could affect the US, pointing specifically to the likelihood Russia will try to use it to evade sanctions and/or establish trade channels and a financial system to operate outside the USD-denominated and Western controlled financial system. Due to notable differences between Russia and the other case study countries, one of the other meaningful sources to mine to look for Russia's foreign and economic policy intent, and for indicators of possible next steps with cryptoruble is Russia's National Security Strategy Until 2020 (NSS RF). The document focuses on and fleshes out the notional of economic security as an element of national security and indeed characterizes economic competitiveness as a principle of national security.[12]

The NSS RF emphasizes the importance of sovereignty as a national goal and states a requirement to "counteract threats to economic security" by executing a socioeconomic policy to ensure sovereignty and shore up the financial system, as well as optimize currency regulation and control.[13] As Kakushadze and Liew characterize it, "Dependence on the existing world monetary order is a major stumbling block for Russia,"[14] and "Russia's ***primary goal*** in issuing a government cryptocurrency is to free their monetary system from the controls exerted by the Federal Reserve (Fed), European Central Bank (ECB) and their allied central banks."[15]

President Putin set the tone for domestic digital technology, when he recommended launching, "a large-scale systematic program of economic development of a new technological generation, the so-called digital economy," and he built on the goal of sovereignty, marrying economic security to national security under the mantle of

digital sovereignty, which cryptoruble is meant to help achieve by the next presidential elections in 2024. According to the General Director of the Zecurion company, Aleksey Rayevsky, "The way, the where, and the how of how this news was announced gives the strong impression that issuing the cryptoruble is more of a political decision than an economic one."[16]

The Kremlin's main proponent for digital sovereignty, Igor Ashmanov, claims, "Digital sovereignty is the right of the government to independently determine what is happening in their digital sphere. And make its own decisions."[17] Ashmanov's fear that, "The introduction of every new technology is another phase in the digital colonization of our country,"[18] fits well into the domestic technology-based cryptoruble narrative, but while digital sovereignty may improve information security – Ashmanov's area of expertise – in a global economy, Russia's "isolationist and authoritarian" digital security doctrine may improve information sovereignty, but it "trumps the [economic] development of the country."[19] The digital economy may provide a means to establish digital sovereignty, but whether it works vice versa remains to be seen. As TRADOC predicts, however, the dynamic of "states defining and defending sovereignty in cyberspace is likely to play out over the next several decades."[20]

The NSS RF alludes to the US and the West by indicating the likelihood of another economic crisis due to "structural imbalances" in the world economy and financial system and pointing to "increased unfair competition, [and] the disproportionate use of legal means" against the RF as having a negative effect on its economic security.[21] It also references "politically motivated sanctions" and use of "economic methods, and financial, trade, investment, and technology policies to solve geopolitical problems,"

stating these actions had weakened international economic relations, although it also asserts Russia's intent to use the full spectrum of "political, information, and financial/economic tools to influence others in the global arena."[22] The NSS RF explicitly calls out the US and its allies, saying Russia's independent domestic and foreign policies cause them to push back because they want to "retain dominance in world affairs."[23]

According to NSS RF, Russia is not focused completely inward, nor does it emphasize Russian exceptionalism, rather, it states its national interests include being a leading world power in a multipolar world. To that end, the document designates the partnership with China as "key to regional and global stability." Regarding the role cryptoruble may play in that partnership, however, while Russia has promoted a multipolar world based on economic might, "China's . . . desire to once again be a regional hegemon and global power,"[24] will likely outweigh any plans for meaningful Russia-China cooperation. The document appears to provide forewarning regarding the messiness of the transition to a multipolar world order, saying it would be accompanied by "increased global and regional instability."[25] This polycentric approach includes building a "full-fledged relationship with the US on points of shared interest, including economic interests," and acknowledges the significance of that relationship on world affairs.[26] A strong Russia-US relationship may be mutually beneficial, considering TRADOC's assessment for the deep future, namely, "the costs of maintaining global hegemony at the mid-point of the century will be too great for any single power, meaning that the world will be multi-polar and dominated by complex combinations of short-term alliances, relations, and interests."[27]

[1] Rose Mahdavieh, "'Governments' Adoption of Native Cryptocurrency: A Case Study of Iran, Russia, and Venezuela" (Honors Undergraduate Thesis, University of Central Florida, Orlando, FL, 2019), 8, https://stars.library.ucf.edu/honorstheses/502.

[2] Ibid., 52.

[3] Ibid., 44.

[4] Ibid., 52.

[5] Ibid., 58.

[6] Ibid., 51.

[7] "Cryptoruble: What is it, Can I Buy it, When Are They Issuing it, and How Can I Use it to Make Money?" Kripto-Rubl, October 24, 2017, https://kripto-rubl.ru.

[8] Ibid.

[9] Orla Ward and Sabrina Rochemont, "Understanding Central Bank Digital Currencies (CBDC). An addendum to 'A Cashless Society – Benefits, Risks, and Issues (Interim paper)'," (Institute and Faculty of Actuaries, London, UK, March 2019), 22.

[10] "Bit-Cohen Brothers: A New Golden Bubble," *Lenta,* August 22, 2017, https://lenta.ru/articles/2017/08/22/bitok.

[11] Ryan L. Frebowitz, "Cryptocurrency and State Sovereignty" (Technical Report, Naval Postgraduate School, Monterey, CA, 2018), 75.

[12] Sergey Bobylev, "Vladimir Putin Signs Updated National Security Strategy of the RF," *TASS*, December 31, 2015, https://tass.ru/politika/2568006.

[13] Ibid.

[14] Zura Kakushadze and Jim Kyung-Soo Liew, "CryptoRuble: From Russia with Love," SSRN, November 2, 2017, 7. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059330.

[15] Ibid., 3.

[16] Igor Serebryaniy, "Why does Russia need the cryptoruble? Experts Are In Disbelief," *Rambler*, October 16, 2017, https://news.rambler.ru/markets/38165540-eksperty-obyasnili-neobhodimosti-sozdaniya-kriptorublya/?updated.

[17] Irina Besedovala, "The Yarovaya Laws Will Save Us from the CIA," *Fontanka*, October 22, 2016, http://www.fontanka.ru/2016/10/22/061/.

[18] Igor Ashmanov, "The Recipe for Digital Sovereignty," *Rossijskoe Agentstvo Novostej*, August 22, 2017, http://www.ru-an.info/.

[19] Lebedev, "Digital Sovereignty."

[20] JCS, JOE 2035.

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Bobylev, "Vladimir Putin Signs."

[26] Ibid.

[27] JCS, JOE 2035.

CHAPTER 4

FINDINGS AND ANALYSIS

The ramifications of the cryptoruble for US national security are: (1) Russia is likely to use it to try to circumvent sanctions; (2) this traceable cryptocurrency provides an opportunity for US national security apparatuses to execute their stated goals, most importantly, defending forward; and (3) current options for addressing this threat will likely be sub-optimally effective because the guidance and resources for addressing it is disparate, and because the US lacks a national economic security strategy to address threats to national security at the intersection of cyber-security and the economy.

Cryptocurrency vs. The Cryptoruble

Cryptocurrency in its "traditional" definition has three primary characteristics: (1) It is *decentralized*, i.e. the information is not held by one organization, such as a nation's central bank, and decisions to approve a payment and move "funds" from one account to another – via a "key" – are made by multiple users, commonly known as "miners". A client/user cannot get their money back if they lose their key because there is no program administrator and there is no way to establish ownership of funds without the key. That also means the currency is not subject to the whims of a government or its international and fiscal policies and actions; (2) Ownership of funds is *anonymous* – the system itself typically does not require any identification to become a member and a user's identity is not identified in any way in the transfers, although a user's identity could still potentially be traced thanks to IP addresses, credit cards numbers used, e-mail addresses used, etc.; (3) Transactions are *transparent and immutable* – once complete, anyone can see from

which account to which account, the amount, and when it was transferred; once complete, there is no way to block or reverse the transfer, although it can be overwritten by a longer chain. Some cryptocurrencies, like Bitcoin, also have a finite emission, which is unusual compared to fiat money.

Blockchain is not the same as cryptocurrency, rather, it is the distributed ledger technology (DLT) on which several cryptocurrencies – including Bitcoin – are based. Blockchain can be used for a wide variety of transactions, not just financial, and has been widely lauded for its ability to speed up administrative paperwork processing, however, that processing currently only happens rapidly (within cryptocurrency ecosystems) because "miners" have a vested interest in rapid processing, in the form of commission. Around the world, several countries have entertained the idea of using blockchain technology within the financial realm, in civic society, and for national security.[1]

Despite being called "cryptoruble", the currency's lack of the most important features of "traditional" cryptocurrencies has been widely recognized: it will not be truly decentralized, which means it will be subject to the government's whims; it will not be anonymous, so the government can track its currency flows; and it will not have limited emissions, rather, the emissions will be controlled by the state. Minister of Communications (MinCom) Nikolay Nikiforov suggested it would be more accurate to call the currency a "digital token"[2], and Deputy Minister of Finance (MinFin) Aleksey Moiseev suggested using, "'cyberruble' instead of 'cryptoruble'" because he felt the state was "creating an electronic ruble, which would just be an electronic form of the paper ruble, perhaps with some expanded uses."[3] But by that time it was too late – the name was too catchy, although, as Alena Narinyani, a journalist and cryptocurrency and

blockchain expert suggests, “the only thing the cryptoruble will have in common with cryptocurrency is the prefix ‘crypto’”.[4]

In examining Venezuela, Russia, and Iran’s approaches, Rose Mahdavieh characterizes this type of financial instrument as a “native cryptocurrency”, and Russia’s proposed version of digital currency would use private blockchain or other DLT, i.e. one that requires permission “from an authorized user to edit and view” the ledger.[5]

Cryptoruble Traceability

Cryptoruble does not just use an encryption that can be broken – and all encryption can be broken[6] – it is meant to be traceable. One of the selling points of traditional cryptocurrencies is that the transactions themselves are traceable, insofar as they are transparent, yet they are not traceable back to an individual if that individual is not linked to the transaction by personally identifiable information (PII) typically linked to a credit card or cryptocurrency market account. Careful traders use mixer programs to ensure none of their PIIs are connected to their transactions, so if a sender or receiver wishes to remain anonymous, they can. By contrast, the cryptoruble will be issued by the government to people who will register with the government, either to convert rubles into cryptorubles or fiat currency into cryptorubles. In the best tradition of post-Soviet propaganda and modern split-screen truth, the anonymity traditional cryptocurrencies afford is “exactly what those lobbying for the idea are counting on”[7] and use repeatedly as an argument for adoption, even though there is no anonymity in a government-issued blockchain. Despite supporters’ fantastical belief that the currency would still be truly decentralized[8], MinCom Nikiforov confirmed there would be no mining,[9] so while the

transactions may still be confirmed by computers solving math problems, the senders and receivers will not remain anonymous, nor will the transactions themselves.

While a blockchain-based cryptoruble will allow the government to trace every user's transactions, the government also has yet to perfect the access to information. As one MinCom representative characterized it, one of the drawbacks to the tool is "the insufficiently developed mechanisms for sharing information and limiting access to information, which could be disastrous if it leaked."[10] While banks may look for a level of interoperability among blockchain systems, the challenge is to create a system that is both efficient and secure. International blockchain standards-setting organizations endeavor to ensure systems which can share information as appropriate, such as in smart contracts in business process management network (BPMN) systems, while also allowing for "enterprise variants".[11] Masterchain, the blockchain currently being developed to serve as the basis of cryptoruble has presented its own challenges in that respect.

Built on the foundation of the popular cryptocurrency Ethereum's blockchain, Masterchain purports to add an additional layer of Russian-government-specific security.[12] The intent is to "grant Russia's monetary system independence from the Federal Reserve, European Central Bank, and allied central banks' control," however, an additional layer could be coded in to "privatize" Masterchain, such that "any funds will be accessible to the Russian oligarchy", ensuring "complete governmental and solitary control over the CryptoRuble."[13] Sberbank is one of the Masterchain developers, and according to Oleg Abdrashitov, head of Sberbank's blockchain lab, the product is "so unreliable that when it enters the production phase, Sberbank plans to use both

Masterchain and the legacy system, so that the experimental tech layer has a secure backup and the operation doesn't collapse."[14]

Assuming the Masterchain developers resolve that problem before rolling out they cryptoruble, other issues remain. Abdrashitov says the system is "not secure" and "for a small network of just a handful of nodes . . . it's easy for one of them to rewrite the ledger."[15] As of 2018, blockchain standard setting was still "both nascent and exploratory" and Ethereum is the only blockchain currently participating, so the foundation of Masterchain is well known and documented. US Cyber Command (CYBERCOM) postures itself to take advantage of such opportunities. According to General Paul M. Nakasone, CYBERCOM Commander, "We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts."[16]

Cryptoruble Slated To Use Nominally Domestic Encryption

Putin married his ostensibly economic idea to the ostensibly national security concept of information sovereignty, alternately referred to in the Russian-language media as digital sovereignty or technological sovereignty. According to Putin, building the digital economy using domestic technology, "is a matter of Russia's national security and technological independence, and in every meaning of the word – our future."[17] In this way he laid the groundwork for rejecting traditional cryptocurrency, while making a "safe" cryptoruble based on homegrown crypto-technologies.

Kremlin sources have echoed this sentiment against foreign crypto-technologies ever since. As Deputy MinCom Sergey Kalugin stated, "Russia needs to maintain its 'digital sovereignty', i.e. not get all fancy with foreign participation . . . The history here

is very important, because if it's all foreign, nothing good will come of it."[18] MinCom Nikiforov has also supported this idea on multiple occasions, calling it "Russia's fate" to create and legalize a domestic system of cryptosecurity (encryption), although critics suggest, "Sovereign cryptography is like the sovereign theory of probability or sovereign algebra, i.e. there can be no such thing."[19]

In an effort to launch cryptoruble effectively, the national security narrative may paper over using Ethereum-based blockchain in Masterchain, founded by Canadian Vitalik Buterin, who is ethnically Russian. Buterin is "actively working with governments around the world,"[20] and Preside Putin reportedly met with him, before ordering the government to develop laws for regulating cryptocurrencies.[21] According to Aleksey Urivsky, a member of the Russian Federation delegation to the International Standards Organization Blockchain Committee, there is not supposed to be any western cryptography in a government cryptocurrency.[22] After some misfires with Hyperledger and consideration of other options, the FinTech Association (AFT), comprised of the Central Bank (CB RF), Alfa-Bank Russia, Qiwi Group, and Vneshtorgbank (VTB, aka External Trade Bank) and, until recently, Sberbank, developed Masterchain.[23] Despite President Putin's direction to launch cryptoruble by mid-2019, Masterchain was released in December 2019.

According to Olga Skorobogatova, Deputy Governor of the CB RF, the CB started working on the prototype in October, 2016, although she did not obligate the CB to a cryptocurrency, instead embracing the blockchain platform as "a component of the new-generation financial infrastructure in the future."[24] The TAdvisor website describes Masterchain as using "Ethereum cryptocurrency" (blockchain) as its base code, "but at

the same time is finished taking into account the requirements of Russian cryptography, user identification process, and secure scaling", while Adbrashitov characterizes it as, "basically public Ethereum's architecture put in a permissioned environment for a closed network of five participants," and has fallen short of expectations for speed and efficiency.[25] Despite AFT claiming its specialization as "cybersecurity and encryption"[26] the reports of Masterchain and cryptoruble's slow and troubled development provides valuable information to the US regarding this (near-)peer adversary's new cyber-economic tool.

Why Cryptoruble is a Threat

The US has recognized the threat to its national security from malign actors using cyber-tools. In 2015, President Obama used his national emergency authority via Executive Order (EO) 13694 to declare, "the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located . . . outside the United States, constitute an unusual and extraordinary threat" and specifically sanction actors who do so "for financial or commercial gain."[27] The ability to use "emerging disruptive technologies" in the context of "rising nationalism, changing conflict patterns . . . and decreasing global cooperation might combine to increase the risk of interstate conflict."[28] This characterization accurately reflects the current state of Russia-US relations, and the cryptoruble as a sovereign cryptocurrency Russia can use to both bypass sanctions and maintain access to all transactions.[29] The combination of Russia's ambition to achieve digital sovereignty – "Russia views cryptocurrency as a means to strengthen its nation and its position in the world,"[30] – and the nebulous

definition within international law of what exactly sovereignty in cyberspace is and thus how it can be infringed or defended[31] result in a recipe for cyber-aggression.

Russia appears to have both the capability and the will to exploit cryptocurrency to the detriment of US national security. According to national security leaders, "Russia is a full-scope cyber actor that poses a major threat" to the US thanks to its "highly advanced offensive cyber program and sophisticated tactics, techniques, and procedures," and Russia's leaders have shown a willingness to use these capabilities against the US.[32] With an increasingly aggressive (near-) peer adversary[33] developing a new cybertools, the question remains as to Russia's tipping point for using it. According to Robert Agnew's General Strain Theory, Russian leaders are likely to commit (cyber) crimes because of their negative affective states, the causes of which include, "(1) failure to achieve positively valued goals . . . (2) disjunction between expectations and achievements . . . (3) removal of positively valued stimuli . . . (4) presentation of negative stimuli."[34] Russia's economy has precipitously declined with the glut of oil and natural gas on the market and an economy lacking any meaningful diversity, combined with US sanctions targeted at Russia's energy sector, leading to sustained financial strain throughout the country and making individual leaders more likely to turn to crime.

Circumventing Sanctions

As the West continues to use sanctions and other financial levers to "disconnect revisionist states [this] will increase their incentive to pursue alternative political and economic arrangements,"[35] and the cryptoruble is one such powerful alternative. Kremlin insiders have suggested the cryptoruble could be "a useful means of avoiding sanctions against Russia and neighboring countries,"[36] including Presidential Advisor Sergey

Glazyev, who gave that as the basis of the "objective need" for the cryptoruble.[37] As he reasons, cryptoruble would allow Russia to do business with financial organizations around the world,[38] although they would still need to do business surreptitiously to avoid secondary sanctions under CAATSA. According to Recorded Future expert Andrey Barysevich, the state could also use traditional cryptocurrencies, and "American and international authorities [would] have an extremely difficult time trying to prove a money transfer was initiated by an organization under sanctions."[39]

The idea of using they cryptoruble to bypass sanctions is in line with countries' observed reaction to sanctions, namely, that they "try to dilute their effectiveness by developing alternative institutions."[40] The cryptoruble may be only one tool in a range of means for mitigating the effects of sanctions. The Brazil, Russia, India, China, South Africa (BRICS) New Development bank may facilitate a supracurrency or just alternative means for payment and financing that cut out the role of the USD by mutual agreement, and the Asian Infrastructure Investment Bank, spearheaded by China and with resources rivaling the World Bank and International Monetary Fund, may serve the same purpose.[41] Multiple observers outside Russia have also drawn the conclusion that not only could cryptoruble facilitate sanctions evasions, it likely will. Already, an official government working group is "investigating possible implementation strategies" to do just that, and Putin's October 2017 rush to establish cryptocurrency regulations could pave the way for the cryptoruble or for the government to investment in traditional cryptocurrencies, either of which could be used to get around sanctions.[42] Once the government makes its own cryptocurrency, it can consolidate power by centralizing the blockchain and coopting what was originally intended to decouple financial transactions

from central banks. Sanctions-busting may even be the primary reason for launching the cryptoruble[43], an intermediate goal to both getting out from under the West's thumb – good for domestic politics – and to establishing a coalition of the anti-West willing.

In an effort to restore its superpower status or at least create a multipolar world to counterbalance the US, Russia is likely to capitalize on any ability it can create to work outside the West's financial bounds, and "the potential of an alliance between Western sanctioned countries, in which Russia is taking the lead, poses a major challenge to US sanctions."[44] In looking for indicators of Russia's likely direction, the focus should be on its leaders, who have the power and the money. Putin's inner sanctum, the so-called 'vertical', has shown a pattern of economic actions furthering their self-interest, rather than improving the national economy, and "Russia's probable intentions behind the development of cryptocurrency is to exert Russian influence globally while exploiting the state and economy."[45] This has led analysts to suggest how oligarchs could benefit from the cryptoruble, both to evade targeted sanctions and to launder any ill-gotten gains. Once they can earn money in cryptorubles, they can use those funds to make purchases, and the money-laundering possibilities became obvious as soon as Russian officials announced there would be a 13% tax on converting funds of undisclosed origin into cryptorubles, a modest business expense.[46] Soon after it was announced, it was apparent the cryptoruble would "allow various individuals and companies to skirt sanctions."[47]

Given the apparent direction cryptoruble will likely take, the effectiveness of US/EU sanctions comes into question. If we overuse them, they lose their effectiveness and drive adversaries to look for end-runs around them, and Russia and China are already "working to reduce their exposure to the US-dominated global financial architecture."[48]

According to Cyrus Newlin, "The perception that sanctions are part of the 'new normal' for U.S. policy toward Russia is likely to encourage and accelerate these efforts—in Russia and elsewhere."[49] And cyberspace is the most likely place for our adversaries to act because they can remain below the threshold of armed conflict while gaining strategic advantage. According to GEN Paul Nakasone, Commander, CYBERCOM, our adversaries "are conducting campaigns to gain cumulative advantage," and "these include efforts to circumvent sanctions."[50]

Using Cryptoruble to Extend Operational Reach in Below-The-Threshold Conflict

On the continuum between peace and war, adversaries often find themselves in competition, which, in itself, ranges from closer to peace to closer to war. With the shift of focus away from counterinsurgency operations (COIN), the US has begun to pay more attention to (near-)peer competitors, who have been "conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage."[51] As they have more success without crossing into armed conflict, US Army Training and Doctrine Command (TRADOC) assumes "adversaries will challenge U.S. interests by means and with ways below the threshold of armed conflict and short of what the U.S. considers war," and cryptoruble is just such a means.[52] The US has remained in the realm of competition with Russia along most vectors for several years, as we find ourselves with "incompatible interests" yet with no desire to resolve those differences via armed conflict.[53] Yet the absence of armed conflict does not indicate the absence of a threat. The US expects its adversaries to parlay their successes in the sub-threshold realm into success in sowing the seeds of discord within the US society. Given the actions

Russia took to interfere in US elections in 2016, cryptoruble appears to be one tool in Russia's multi-layered standoff, the use of "diplomatic means, economic levers, unconventional warfare, information operations, and conventional forces" to "create political separation".[54] If the US hopes to keep Russia's success in the competition space to a minimum, it must engage in deterrence in the competition space "to counter the malign influence . . . from Russia"[55], although it is more challenging in the sub-threshold operational environment.[56]

The primary domain for these sub-threshold operations is cyberspace. While activities in the cyber domain do not limit the US' response to cyberspace, the US is cognizant of proportionality, so states will continue to use cyber tools to "to augment their power, degrade or usurp the power of others, and gain strategic advantage through competition."[57] The persistent interconnectedness of cyberspace allows adversaries to conduct a continuous campaign producing "cumulative, strategic impacts by eroding U.S. military, economic, and political power."[58] Russia has proven a dangerous pacing threat, demonstrating its intent to drive a wedge between the US and its partners in Georgia and Crimea/Ukraine by engaging in armed conflict that stops short of provoking an armed response.[59] As Russia continues to enjoy success in the sub-threshold range on the competition-conflict continuum, "the next logical step will be to invest in the capabilities necessary to assert themselves even farther from their borders . . . [and] the leading edge of this new global reach will be investments in more advanced cyber capabilities."[60]

Below-the-threshold activities within the cyber realm square nicely with Russia's asymmetric approach to modern warfare along the conflict continuum.[61] According to Deputy Minister of Defense A.V. Kartapalov, Russia's approach to modern conflict

requires a "hybrid war" approach, including "taking political, economic, information, and psychological actions against the adversary."[62] Kartapalov takes his cue from British military theorist Liddel Hart, who advocated for a strategy of using indirect actions "to suppress the adversary's resistance" because they are "more effective at breaking the psychological and physical stability of the adversary, thus creating the conditions for his dismantling."[63] What Russian military theory now refers to as "new war", is a state of continuous competition, ranging from closer to collaboration to closer to hot conflict, a war that is "never declared and is never over."[64] For Russia, "wars have become economic, financial, cultural, and . . . hybrid"[65] and planners have turned their focus to developing non-kinetic tools such as the cryptoruble, which they can use as a tool for economic manipulation to circumvent sanctions and thus chip away at the American will. Based on recent Russian conduct, the US can expect Russia to continue its layered stand-off across the political, economic, and military arenas[66] and try to increase its global profile and influence.[67]

Russia and China As (Near-)Peers

As the familiar rules-based world order of the late 20th century has started to change, "China and Russia prove the most capable . . . among the states most likely to contest international norms."[68] While China may be strong enough to challenge the status quo, Russia can also exploit strained Western alliances in pursuit of its own form of "'strategic self-determination'".[69] As post-Soviet politicians have often stated, "We have our own democracy," and in the 21st century Russia has continued to insert itself between the US and Europe, counting on Europe's energy dependence on and proximity to Russia as a mitigating factor to any economic or political retaliation. Like Russia, China has

made an effort to free itself from foreign technology (see Program 863) and "sees cyberspace as a way of compensating for its deficiency in conventional warfare" because it can extend its operational reach to US systems in the cyber domain.[70] As both Russia and China hone their cyber capabilities, they will "pose increasing threats to US . . . economic prosperity, and stability,"[71] both of which the National Security Strategy (NSS) calls on the nation to defend.[72]

One of Russia's primary targets has been challenging the US in the economic sphere and the two countries are likely to remain in the range of competition as the two countries' goals and priorities continue to conflict.[73] Both Russia and China have already proven their ability and intent to engage in "economic espionage" against the US[74] and they are now creating operational and strategic stand-off capabilities.[75] The advantage of stand-off is having the "freedom of action . . . to achieve strategic and/or operational objectives before an adversary can adequately respond,"[76] and as Russia develops that, it can use economic/information/diplomatic means to isolate the US and drive the wedge further between the US and its allies and partners.

Cryptoruble of Concern for the Intelligence Community, Not Just for Department of the Treasury

In the Russian concept of information warfare, cyberoperations are just one weapon in the arsenal, and cryptoruble could be considered an information weapon, insofar as Russian authorities may use it to produce data to accomplish a mission.[77] As the US economy becomes more digital and Russia nears its own digital economy goals, "the threat to national security is significantly increased," and Russia has already demonstrated a willingness to conduct a cyberattack against the financial systems of

Estonia, a NATO ally.[78] As the Director of the Defense Intelligence Agency testified in 2019, "We expect disruptive cyberactivities to be the norm in future political or military conflicts," and "we must develop flexible capabilities" to counter each adversary's specific intent.[79] In 2012 the Director of National Intelligence rated cyber threats as the third most dangerous to national security, behind only terrorism and proliferation, and the Intelligence Community (IC) predicted US adversaries would continue to exploit the cyber domain to increase competition and standoff capabilities.[80] The IC works to expand US competitive capabilities, to provide policymakers with "effective options for operational cyber responses to threats to U.S. interests."[81]

Using a DIME Approach

The US combines diplomatic, information, military, and economic (DIME) tools to address threats to national security. It uses "all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten U.S. national interests, our allies, or our partners."[82] The DIME approach includes applying military resources along the range of competition, and the US works to deter adversarial actions using means that remain below the threshold of armed conflict. As Russia acts to extend both its operational reach and its standoff capability using information "warfare" in the sub-threshold range, so the US uses a combined approach, which may apply Department of Defense (DoD) and IC resources without ever having to use conventional weapons (see figure 2 below). With its own effective layered standoff, the US can deter adversarial acts of aggression in the cyber domain by using "***rapid and continuous integration of all domains of warfare*** to deter and prevail as we ***compete*** short of armed conflict."[83] The DoD and IC bring significant resources to bear, especially the

DIRNSA/CHCSS, as the "DoD focal point for cybersecurity cryptographic research and development,"[84] and the *U.S. Army Concept for Multi-Domain Combined Arms at Echelons Above Brigade, 2025-2045* calls for Army forces to "provide essential linkage to the expanded instruments of national power" and "operate ubiquitously with joint, interagency, and multinational partners to overmatch any threat in any future environment."[85] So while a joint force solution may constitute the primary effort, the intent is to "defeat the adversary's efforts to achieve their strategic goals" in the competition space and "it does this by expanding the competitive space for policymakers through multiple options for employing the elements of national power."[86]

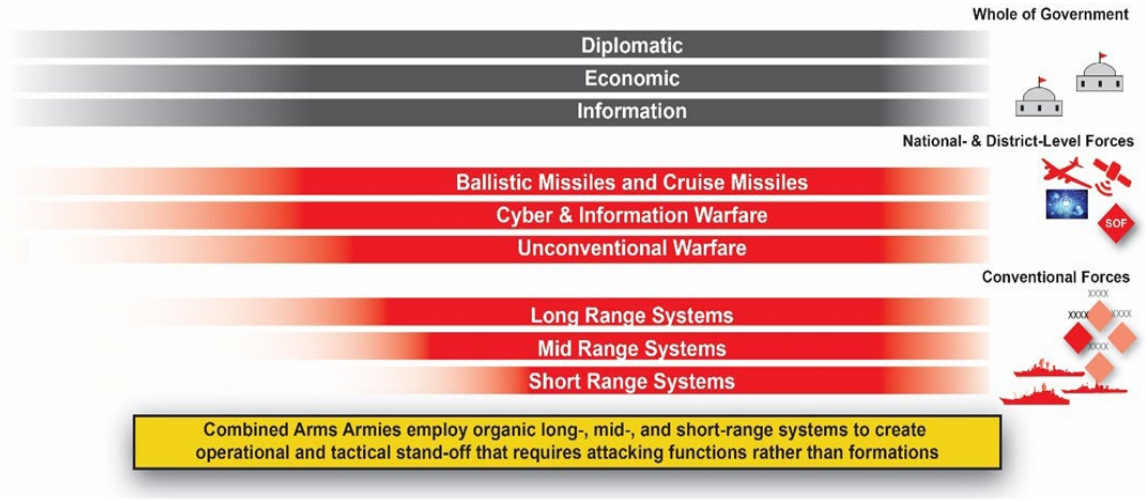

Figure 2. Adversary's Layered Stand-off

Source: U.S. Army Training and Doctrine Command (TRADOC), TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 2018), 12.

As part of "supporting strategic competition," CYBERCOM is well suited to lead the effort to deny Russia's ability to use the cryptoruble against US national interests, as

"it acts against adversaries who can operate across the full spectrum of cyberspace operations and who possess the capacity and the will to sustain cyber campaigns against the United States and its allies."[87] CYBERCOM itself works with the rest of the IC, other federal agencies, and has been partnering with industry partners in finance.[88] As the newest domain in multidomain operations, members of the cyber community continue to advocate for integration, and see cyber deterrence as part of a greater cross-functional effort, including using "diplomatic demarches, sanctions or indictments,"[89] among other DIME tools. The DoD Cyber Strategy requires the department to work with "other departments and agencies, as well as with our allies and partners" to "expose, disrupt, and degrade cyber activity threatening U.S. interests," including activities that affect the US economy.[90]

A Proactive Approach to the Cryptoruble

According to Routine Activities Theory, the crime rate depends on the "availability of targets" and the "absence of capable guardians".[91] Russia has already demonstrated its intent to engage in information warfare against the US and US/EU sanctions are an available target. The target also needs to be suitable, i.e. sufficient value, few enough obstacles, visibility of the target, and ability to easily access the target and exit.[92] Using cryptoruble in the cyber domain would allow Russia the ability to circumvent sanctions one deal at a time, via electronic access, while publicly embarrassing the US if it became public, and getting access to sanctioned technology if a seller accepts the payment.

The US can avoid such "strategic surprise" if it invests in planning for deterrence early and takes a national-level approach.[93] The Director of National Intelligence

identified cyber threats as posing "critical national and economic security concern" and both state and nonstate actors are improving their capabilities.[94] Without a proactive approach, Russia can leverage its standoff to its advantage.

In planning for the future, the Multi-Domain Operations (MDO) Concept focuses on "active engagement by the Joint Force" because "in the past, the US military . . . has often remained reactive in competition below armed conflict."[95] That approach is now codified in the DoD Cyber Strategy, requiring the DoD to "defend forward, shape the day-to-day competition . . . to compete, deter, and win in the cyberspace domain,"[96] and defending forward requires the US to stay ahead of its adversaries "both in knowledge and in action."[97] Planning now to meet the challenge of the cryptoruble will require engaging multiple tools in the US toolbox, and given the level of US exposure, the US cannot afford inaction.[98]

To avoid creating a "norm of inaction"[99] when Russia does not respond to sanctions, the US has added other approaches. In 2019 President Trump suggested a "US-led 'deterrence initiative' that includes collective response to malicious cyber activities by China, Russia, Iran and North Korea",[100] while Timo Koster, Netherlands Ambassador-at-Large for Security Policy and Cyber, called for a framework . . . to "both overtly and covertly react to malicious behavior."[101] Given the relatively nascent stage of cryptocurrency development, and especially national cryptocurrency development, now is the time for the US to "develop its own capabilities within the digital economic environment to protect U.S. national interests in the future."[102] If the Joint Force takes an active engagement approach to cryptoruble, as it does in regards to other adversary actions in the competition space, it can make a "robust operational assessment of the

adversary's forces and capabilities,"[103] the electronic equivalent to making contact with the enemy as a form of reconnaissance. Getting ahead of the cryptoruble before it is used to circumvent sanctions gets the US inside Russia's OODA loop (observe, orient, decide, act), and defeating destabilization efforts sub-threshold is the most effective approach the US can take.

Tracing Cryptoruble Flows

CYBERCOM's 2018 shift in focus to "stopping cyber threats before they hit the United States was soon hailed as a marked shift" in US strategy.[104] One of the greatest challenges the US faces in countering adversaries in the cyber domain is the ability to attribute attacks and locate the perpetrators in real time.[105] The US has and is developing a variety of tools and approaches to meet those challenges. In the age of data pools and automated processing, using algorithms to process large volumes of data could give the US both "situational awareness and decision-making advantage,"[106] and the US could also deter adversarial actions by denial.[107] Once the US can trace cryptoruble flows, it has multiple legal options for what to do with the information. Once it has identified these cyber actors, it can shadow them to "keep them constantly on-guard and off-balance" and it can also "signal their national leaders that attribution and response to cyber aggression will be swift."[108] It could also attempt to directly influence cyber operators, as it did with Russian cyber operators identified as interfering in US elections.[109] To remain legal, the US must take care not to harm data or networks as part of its deterrence efforts[110] and, at the same time, cyber deterrence is but one tool in US deterrence toolbox[111]; the US relies on its policies, strategies, and international law to determine proportional responses.

The Authority to Act

In pursuit of defending forward in the cyber realm, the IC has legal foundation to collect intelligence on "important targets overseas" in Title VIII of FISA.[112] Within the US Army, several organizations support cyber efforts. The Commanding General of Army Materiel Command (CG, AMC) is responsible for managing "cryptographic and key management technology exploration and validation activities in support of the Army CIO/G–6."[113] The CG, Army Intelligence and Security Command (INSCOM) works together with the Army CIO/G–6, DCS, G–2, ARCYBER, and Criminal Investigation Command (CID) to analyze "foreign intelligence threats . . . and operational vulnerabilities against which cyber-security counter-measures will be directed."[114] Once CYBERCOM established "defend forward" as its guiding operational concept in 2018, the US raised the profile of cyber security to a national priority and prioritized the DoD as the leader in the US strategy of persistent engagement to "inhibit incessant adversarial cyber operations against the United States."[115]

US Policy Foundation for Addressing Cryptoruble

National Security Strategy (2017)

The National Security Strategy (NSS) of the US is the primary strategic guidance for all government organizations, with multiple more specific strategies nested with it, to provide more granular guidance to execute the plans as laid out from the top. Pillar II of the NSS establishes, "economic security is national security"[116] and Pillar III establishes the requirement for diplomacy and statecraft capabilities and, within that, the capability to use tools of economic diplomacy to defend against "threats from state-led economies"[117]. Specifically, the NSS provides guidance via its priority actions to "deploy

economic pressure on security threats" and "sever sources of funding".[118] This means the US, its allies, and partners must maintain the will to impose and enforce sanctions against nations to shape their behavior in ways beneficial to national and international security.

The US can sever funding using tools other than sanctions, however, and the NSS points to success in the competition space to as "the best way to prevent conflict."[119] In addressing what the DNI identified as one of its greatest challenges, the NSS pledges to increase US capability to expand its awareness of malicious cyber activities and identify cyber attackers. The NSS recognizes the key role cyberattacks play in modern warfare, especially to project influence and power, and pledges to deter, defend against, and defeat malign actors using cyber capabilities,[120] just as it would those using other attack capabilities. Most importantly in regards to the capabilities the cryptoruble affords, per NSS guidance, the US will take worthwhile risks in response to cyber threats[121] and will "pursue new economic authorities" to increase its options to create economic pressure.[122]

National Intelligence Strategy (2019)

The National Intelligence Strategy (NIS) provides guidance to the intelligence community (IC), a collection of 17 different organizations including DoD and other government agencies, whose collective principles include achieving an "exquisite understanding of our adversaries' intentions and capabilities."[123] One of the IC's primary objectives is strategic intelligence, which includes developing a "deep understanding" of both state and non-state capabilities and intent, to provide warning of upcoming developments to help US leaders in making national security policy and strategic decisions.[124] To achieve this objective, the IC must continue to develop new tools to

gather and evaluate information to track changes within global operational environment, across political, diplomatic, military, economic, security, and information domains.[125]

National Cyber Strategy (2018)

The National Cyber Strategy (NCS) provides guidance to all federal organizations operating within cyber space. The President issued this strategy just nine months after issuing the NSS and the NCS picks up and develops the threads of NSS related to protecting national security and prosperity, as "Ensuring the security of cyberspace is fundamental to both endeavors."[126] Echoing the NSS, the NCS views economic safety as hinging on national security[127] and vows to use its cyber capabilities to both advance US interests[128] and to achieve national security objectives.[129]

The US has been the sole global super power since the decline of the Soviet Union, but according to the NCS, "this now-persistent engagement in cyberspace is already altering the strategic balance of power."[130] The NCS sees US adversaries as hiding behind "notions of sovereignty" while engaging in "malicious cyber activities, causing significant economic disruption,"[131] and Russia justifies its cryptoruble effort, in part, by claiming it will help the country achieve 'digital sovereignty'. Cyber space is a domain in which the US can create consequences for behavior deemed harmful to the US and the NCS calls on leaders to use "diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities," to do that.[132] In addition to its own national interests, the US may eventually take an interest in "exposing and countering repressive regimes' use" of the cryptoruble to "undermine human rights"[133], because the Russian government can make cryptoruble the sole legal

form of payment, in which case they can trace individuals' purchases and even exclude them from the economy at their whim.

Key to the US cyber strategy is integrating cyber tools "across every element of national power"[134] and, notably, into partner-based approaches, with consequences for harm to US allies and partners as well.[135] This is part of the whole-of-society approach espoused in the NCS, namely, that federal government agencies will accomplish their cyber goals by "working with foreign government partners as well as the private sector, academia, and civil society,"[136] namely because US allies and partners have complementary skills, resources, and capabilities.[137] President Trump's international Cyber Deterrence Initiative was first proposed in the NCS and as federal agencies, allies, and partner work to identify hostile foreign nation states, and non-nation state cyber programs, intentions, capabilities, research and development efforts, tactics, and operational activities"[138], they may be able to uncover other malign actors, i.e. those who accept cryptoruble for payment and what they are willing to sell.

DoD Cyber Strategy

The DoD Cyber Strategy reinforces the assertion made in the National Defense Strategy[139] and NSS, that the US is "engaged in long-term strategic competition with China and Russia,"[140] and the best way to deter and defeat is to do so in the competition phase. Active competition and deterrence are "mutually reinforcing activities"[141], and for operations in the cyber domain, that means shaping the operational environment on the daily.[142] To compete successfully against the cryptoruble, the DoD will have to realize its goals to "accelerate cyber capability development"[143], cultivate talent, and conduct its own internal reforms.[144]

The Purpose of Sanctions

The US uses three tiers of sanctions: asset freezes, visa bans, and economic sanctions – tiers one, two, and three, respectively[145] – to "punish opponents and reshape behavior."[146] Economic and financial sanctions can be particularly powerful when levied by the most powerful economy in the world, and when the economic powerhouses of the US and EU jointly levy sanctions, the stakes for violating them are high. The role of the USD as the global reference currency and the significant role of the Society for Worldwide Interbank Financial Telecommunications (SWIFT) bank transfer system make US sanctions a meaningful instrument of foreign policy and national security.[147] The US uses economic sanctions as "coercive economic measures" which may include "restrictions on particular exports or imports", and "prohibiting transactions involving U.S. individuals and businesses",[148] and which may slow a target country's economic growth.[149] If Russia can convince another entity to accept cryptoruble as payment for a technology whose import the US has sanctioned, the US may levy secondary sanctions against that third party, specifically because they helped Russia find a way around US sanctions.[150]

Several federal agencies participate in implementing economic sanctions, most important of which is the Department of Treasury's Office of Foreign Assets Control (OFAC), which curates the Specially Designated Nationals (SDN) and Sectoral Sanctions Identifications (SSI) lists. The OFAC can limit individuals' and entities' ability to access assets, the US financial system, import and export licenses, investments, and trade deals, among other things.[151] The Department of Commerce's Bureau of Industry and Security (BIS), which "restricts licenses for commercial exports, end users, and destinations,"[152]

and the Department of Justice, which investigates sanctions violations,[153] also play important roles.

The Role of the US Department of Treasury

The Treasury Department researches and analyzes economic developments worldwide and helps set economic policies.[154] Within Treasury, the OFAC is responsible for administering and enforcing economic sanctions "based on US foreign policy and national security goals" vis-à-vis the countries, entities, and individuals targeted. Malign actors may threaten the US economy, foreign relations, or national security, and sanctions may be Congressionally mandated, UN mandated, based on some other multilateral mandate, or Presidentially directed by Executive Order.[155] Most US sanctions against Russia are not against the government, but against select entities the OFAC has listed on the SDN, "and generally prohibit U.S. individuals and entities from engaging in transactions" with those entities.[156]

In addition to OFAC, Treasury has a separate bureau called FinCEN, focusing specifically on cryptocurrencies and "responsible innovation", to protect national security.[157] According to FinCEN Director Kenneth Blanco, regulations pertaining to transmitting fiat currencies apply to cryptocurrencies as well.[158] He also emphasized the importance of public-private collaboration in developing methods to "identify, track, and stop . . . bad actors . . . from coopting innovation and technology" to use against the US[159], raising the separate possibility of a third party that could itself infiltrate cryptoruble and use it for nefarious purposes, regardless of Russian leaders' intent.

Current US Sanctions Against Russia

In the modern, post-embrace era, Russia has actively postured itself in a neo-Cold War stance by engaging in sub-threshold provocations to (re-)create a worthy opponent and get the US to push back, and "many observers consider sanctions to be a central element of U.S. policy to counter Russian malign behavior."[160] Putin first found populist support in this stance, then consolidated his power using a classic Soviet combination of a stranglehold of domestic society combined with fear-mongering regarding Western powers. The US Congress has pushed back with robust sanctions passed throughout the 115th Congress (January 2017-January 2019), most notably through the Countering Russian Influence in Europe and Eurasia Act (CRIEEA), Title II of the Countering America's Adversaries Through Sanctions Act (CAATSA), which "codifies Ukraine-related and cyber-related EOs [executive orders], strengthens existing Russia-related sanctions authorities, and identifies several new targets for sanctions. It also establishes congressional review of any action the President takes to ease or lift a variety of sanctions."[161] Some of these sanctions are punitive, while others aim to "deter further objectionable activities"; some specify behavior to engage in, e.g. abide by the Minsk agreement ceasefire in Eastern Ukraine, and others behavior to avoid, e.g. cease malicious cyber activity, and cease supporting the Syrian and North Korean regimes.[162] From 2012-2018, the US has imposed "more than 60 rounds of sanctions" against Russia,[163] primarily for human rights abuses, the invasion of Ukraine, and interference in US elections, all of which CAATSA reiterated and reinforced, as well as adding sanctions for corruption and malicious cyber activities more broadly.[164] Of all the current

US sanctions against Russia, the majority were "levied in response to Russia's 2014 invasion of Ukraine."[165]

In March 2014, the US declared sanctions against Russia for threatening the "peace, security, stability, sovereignty, and territorial integrity of Ukraine," annexing Crimea, and a litany of accompanying violations of international norms.[166] These sanctions include three basic types: blocking (so US entities cannot do business with them), sectoral (banking, energy, and Arctic exploration-related technology), and investments and trade with entities in Crimea.[167] Their objectives are clear: enforce compliance with the Minsk Agreement and deter further Russian aggression.[168] What good looks like remains elusive, however: while compliance with the ceasefire is verifiable, at what point does the US declare Russia does not intend any further aggression? The Ukraine-based sanctions, moreover, were intended to have only a limited impact on the Russian economy overall, and instead "target individuals and entities responsible for offending policies and/or associated with key Russian policymakers in a way that would get Russia to change its behavior while minimizing collateral damage to the Russian people or to the economic interests of the countries imposing sanctions."[169] While the US and EU have put in place "mutually supporting" Ukraine-based sanctions, including limiting financial transactions and access to capital markets, targeting energy companies and companies linked to President Putin, limiting military and defense cooperation, and imposing secondary sanctions,[170] their efficacy remains in question.

Upon signing CAATSA into law, President Trump called the legislation "significantly flawed" and in some places "unconstitutional" and suggested he would

finesse the implementation as part of engaging in foreign relations.[171] In its Kremlin Report of January 2018, however, Treasury reserved the right to list 210 individuals close to Mr. Putin, including the top 25 richest people in Russia, directors of state-owned companies, members of Mr. Putin's administration, and his security detail, commonly referred to as his henchmen.[172] As of January 2019, Mr. Trump had added 29 new designations, 24 of which were cyber-related, but no new secondary sanctions, commonly used to punish sanctions evasion.[173] OFAC, however, added 13 companies in the finance, energy, and defense sectors to the SSI,[174] significantly including Sberbank and VTB, both of which worked on the Masterchain cryptoruble project; and Gazprombank, which, together with VTB, invested heavily in developing Venezuela's national cryptocurrency, the Petro.

The sanctions that "seek to impose costs without being linked to a specific policy outcome," many of the CAATSA (2017) and "oligarch sanctions (2018) provide only broad mandates to stem malicious cyber-enabled activities and prevent oligarchs from profiting by corrupt means.[175] According to Cyrus Newlin of the Center for Strategic and International Studies, "There is no instruction on the steps necessary to lift these sanctions, perhaps indicating an assumption on behalf of U.S. policymakers that the behavior of the sanctioned entities will continue."[176] Meanwhile, the sanctions preventing Russian companies from getting Western technology to modernize their oil and gas industries, were intended to inflict a slow burn, and "The full economic ramifications of these restrictions potentially have yet to materialize."[177]

Sanctions will likely remain one of the most important tools for the West to shape Russian behavior.[178] If the US can trace cryptoruble flows, it may be able to catch Russia

in violating sanctions against malicious cyber-enabled activities, especially for financial or commercial gain[179], or a double violation of that and acquiring energy industry technology, for example. The question remains the teeth behind the sanctions: if the consequences for sanctions violations are inconsequential, sanctions are insufficient for the West to get the behavior it wants from Russia.

Effectiveness/Ineffectiveness of Sanctions

General Effectiveness

The importance of sanctions has grown as security threats have increased, and they are all the more important as the US and its allies have become less and less willing to engage in armed conflict,[180] especially with a (near-)peer adversary. The effectiveness of sanctions comes not only in convincing the target country to change, but in convincing other countries to abide. Sanctions-busting can be quite profitable for companies in the sanctioning country willing to take the risk or for third-party countries[181] unwilling to support sanctions,[182] especially if the third party is not a signatory and considers the risk of secondary sanctions worthwhile.

Already, "a significant amount occurs openly between third-party and target states through legitimate channels when third-party governments refuse to cooperate in imposing sanctions."[183] For sanctions to be effective, the US and EU must keep in mind other countries' calculus, including trade, banking, and commercial interests, as well as their foreign policy goals.[184]

What Makes Sanctions Effective or Ineffective?

The US has several examples to look to for guidance as to what makes sanctions relatively more or less successful. One clear pattern is the power of multilateral sanctions: the UN Security Council sanctions against Iraq (1990-2003) were "effective at crippling the Iraqi economy because they were enacted and enforced by an essentially global coalition".[185]; the sectoral sanctions imposed by the Coordinating Committee for Multilateral Export Controls (COCOM, predecessor to the Wassenaar Arrangement) severely hampered the Soviet Union's ability to acquire new technology throughout the Cold War.[186], thanks to a multi-country effort. Sanctions have been even more effective when they are both multilateral, and affect a significant part of the economy, for example, denying access to the SWIFT system, which "facilitates most cross-border payments in the world."[187] Such sanctions against Iran (2010-2013) helped slow the country's economic growth (0.2% per year compared to 1.7% worldwide and 2.3% in the Middle East and North Africa) and Iran subsequently returned to negotiations.[188] Sanctions make a bad economy worse, as countries like Venezuela show, where hyperinflation in the context of sanctions have sent the economy into a tailspin.[189] While there is no definitive direct causation between sanctions and economic failure, there is a correlation, and economic sanctions do magnify existing economic woes.

By itself the US can effectively "exclude entities from the formal global financial system".[190] because so many global financial transactions go through US banks who have no incentive to transact with sanction incompliant banks, but the US is not the only economic powerhouse in the world. Once the US pulled out of the Joint Comprehensive Plan of Action (JCPOA), that left China, Russia, France, the UK, and Germany still in the

nuclear program agreement with Iran, and China decided to use its power as the world's largest crude oil importer to its advantage.[191] While its Iranian imports dropped significantly after the US re-imposed sanctions against Iran, China remains Iran's biggest oil consumer[192] and China has brokered deals denominated in renminbi (RMB, i.e. yuan), a significant departure from most deals, which are denominated in USD. Meanwhile Iranian President Rouhani suggested a Muslim-country trade zone, encouraging countries to conduct trade in their own currencies,[193] reinforcing the fact that no country is legally obligated to make deals in USD or uphold US unilateral sanctions.

While economic sanctions remain an important tool for the US, the US cannot rely on them to reach its goals, even when the targeted country has a significantly smaller economy, e.g. as happened in Haiti and Panama.[194] Only 13% of US unilateral sanctions levied 1970-1997 achieved their stated foreign policy goals,[195] and unilateral actions 2017-2019 have created concern among members of the EU regarding future sanctions coordination with the US, especially regarding the situation in Ukraine.[196] Moreover, the conditions that make an OE more conducive to unilateral sanctions – modest goals, a significant power differential between the players, and a substantial trade relationship prior to sanctions[197] – do not exist in the case of the US and Russia. Executing the Minsk Agreement, ceasing malicious cyber activity, curbing corruption, and slowing growth in the energy sector are hardly modest goals, Russia is a (near-) peer competitor, and Russia had a more robust trade relationship with the EU than with the US prior to the new round of sanctions starting in 2017.

Russia has already demonstrated sanction workarounds: "the Kremlin-controlled Russian Direct Investment Fund has actively courted investment from other sovereign

wealth funds, including from the Gulf States," and the Central Bank has offered "correspondent banking access, should Washington revoke these privileges with future sanctions.[198] A 2007 review of 174 sanction cases showed even multilateral sanctions are most likely to succeed when they have limited goals; "sanctions aimed at regime change or to cause major policy change sometimes worked; and sanctions to disrupt minor military actions worked least often."[199] In addition, sanctions must specify the conditions for lifting them,[200] otherwise, they cannot be deemed effective or ineffective. The more sanctions appear to the target to be politically motivated, the more targets will look for ways around them,[201] and the more they seem "permanent and inevitable," the more likely the target will be to just live with them, rather than work to get them lifted.[202] "Sanctions work best when they provide leverage. Overuse of sanctions . . . particularly those not linked to concrete policy objectives, generate little leverage and help entrench Russian views that the ultimate goal of U.S. policy is less behavioral change than regime change,"[203] and this makes the current set of sanctions against Russia look unlikely to succeed.

Effectiveness of Sanctions against Russia

It is unclear how sanctions since 2012 have changed Russian behavior,[204] which shows that sanctions may have the desired effect of weakening the Russian economy or a specific economic sector, or of economically punishing specific individuals, however, that effect does not necessarily translate into the overall goal of sanctions, namely, to change Russian behavior. Some sanctions have overshot the mark, causing more economic disruption than intended. The sanctions against aluminum company Rusal "had broad effects that rattled Russian and global financial markets", due to the size of the firm

– one of the top 20 countries in Russia and the second largest aluminum manufacturer worldwide – and OFAC's signal that it would actually impose the secondary sanctions required by CRIEEA.[205] The now real threat of secondary sanctions "attracted international attention and made foreign banks and firms reluctant to engage in any transactions with Rusal."[206] The unintended effect of this sanction against a Russian company was economic instability in the global financial markets, so OFAC agreed to remove the sanction "on the basis of an agreement that would require Kremlin-connected billionaire Oleg Deripaska . . . to relinquish his control over the firm."[207] OFAC counted this as a win, saying they had reached their goal of economically punishing this one oligarch, however, other observers characterized the incident as demonstrating the "limits to U.S. resolve on sanctions."[208]

While the effects on the Russian economy overall has been relatively mild, certain firms and sectors showed a more significant economic effect: Russian banks have been reluctant to provide services in Crimea – likely more detrimental to Crimeans than to Russians – and Western oil companies have limited their involvement in Russia and with Russian companies, limiting Russia's access to new oil technology.[209] Meanwhile, other firms are more profitable now than they were when sanctions were originally levied on them in 2014, including Sberbank (the largest bank in Russia), Rostec (a major defense conglomerate), and Novatek (an independent natural gas producer).[210] Economic sanctions may have "caused a significant drop in the living standards of many Russian citizens,"[211] nevertheless, the personal effects seem to have hit oligarchs harder, and OFAC has reached some of its goals as its sanctions "have already cost many of Putin's supporters in the business community a significant part of their wealth."[212]

With no specific metrics, sanctions such as the anticorruption oligarch sanctions and those meant to deter future bad behavior, such as curbing malicious cyber activity, are hard to judge as successes or failures because they are not linked to specific behaviors to reverse or engage in as proof.[213] Perhaps the OFAC can determine some signs of success in Russia's seemingly desperate acts of forming closer ties with other sanctioned countries, especially Venezuela, and creating their own cryptocurrency.[214] Sanctions against Russia have had an indirect effect on its economy and sanctions against specific companies have had an indirect effect on other companies in the same sector, especially in the banking/financial sector, which depends heavily on faith in the economy for outside funders to invest.[215] That fear may be the most lasting effect of Western sanctions and underscore the phenomenon of sanctions adding to an already bad economy. The secondary effect of Russian banks losing outside investment is that they become more dependent on the CB RF, which centralizes Kremlin control even further. This boomerang effect begs the question, What type of Russia does the West really want? The US and EU want to slow Russia's economic growth, but "the collapse of the Russian economy would not be in the interest of the West."[216] For several years, the West was trying to bring Russia into the fold, and supported its economic growth as Russia demonstrated a burgeoning democracy, but Russia could not break its political and economic centrifugal force, and now the best the West can hope for is "an aggressive but weak Russia", i.e. containment.[217]

Even the sanctions whose requirements can be demonstrably met have not been: Russia has not stopped its activities in Eastern Ukraine and has, in fact, expanded its military activities in the region.[218] Despite significant sanctions since 2011, Russia

appears to have come to terms with them as the never-ending status quo, an annoyance to live with and work around, not a catalyst for change.[219] What remains to be seen is how Russia will behave as the sanctions weigh down an already heavily burdened society. Alone, "the economic impact of sanctions may not be consequential enough to affect Russian policy,"[220] but the economy has several weak spots it has not been able to shore up over decades: the financial success of the country is based on its oil and gas riches, so while sanctions have denied Russia access to Western technology for modernization, even more harmful has been the falling price of oil, ostensibly due to part to increases in US production. Russia's failure to diversify the economy was not for lack of effort: President Medvedev made several valiant attempts, including establishing Skolkovo, the "Russian Silicon Valley", but he could not push through political reform and accomplish his stated primary goal of stemming corruption, and President Putin only made the situation worse upon his return to the presidency.[221] As the economy spirals downward, internationals investors are "unwilling to roll over maturing debt" and Russia is forced to "run down foreign currency assets to cover the difference," but two sovereign wealth funds hold almost half the reserves,[222] concentrating political and economic control along Putin's 'vertical' now more than ever.

Although it is nigh on impossible to establish cause and effect with sanctions due to the other ongoing economic challenges Russia faces, the Russian government openly acknowledges their detrimental effect. Russian Finance Minister Anton Siluanov noted their contribution to a weakening economy[223] and the government even called on Russian elite to repatriate funds from their offshore accounts to stem the tide of capital flight.[224] While "many observers argue that sanctions help to restrain Russia or that their

imposition is an appropriate foreign policy response regardless of immediate effect,"[225] economic and financial sanctions 2012-2019 cannot be characterized as effective in changing Russian behavior.

How Russia Responds to US and EU Sanctions

During the Russian recession of 2014-2015, a perfect storm of a plummeting ruble, capital flight, and runaway inflation, US sanctions added insult to injury by denying sanctioned companies access to capital markets, while other companies in the same sectors also often suffered guilt by association.[226] In response, the government let its deficit grown and tapped its capital reserves, investing federal funds into sanctioned companies by awarding them key contracts: Bank Rossiya (CB RF) won the sole contract to service the domestic wholesale electricity market, Storygazmontazh won the contract to build the bridge between mainland Russia and Crimea, and VTB won the contract to be the sole manager of federal international bond sales.[227] CB RF propped up banks by buying the debt they could no longer sell, as well as providing loan forbearance, and access to foreign currency; the government increased its orders from sanctioned defense firms and nationalized and repurposed Promsvyazbank specifically to finance defense firms; and that same bank even extended a line of credit to oligarch Viktor Vekselberg just weeks after he and his company were sanctioned in 2018.[228] This federal support mitigates the effects of sanctions and is expected to continue: "The government is creating a department within the Finance Ministry to liaise with sanctioned businesses, study their challenges, and draft government proposals for support."[229]

Like other repeatedly sanctioned countries, Russia is now incentivized to find alternatives, be it by alternative agreements, using traditional cryptocurrencies, or

creating its own cryptocurrency, to decouple its economy from the world financial system.[230] In November 2016, President Putin bemoaned the effects of sanctions, in July 2017 presidential economic advisor Aleksey Kudrin said they were "preventing the country from regaining its status as a leading economic power,"[231] and by October 2017, the cryptoruble was announced as part of the Digital Economy platform, and lauded as a way for Russia to gain digital sovereignty.

Meanwhile, Russia could help its situation by exploiting the growing rift between the US and its allies to determine a way forward with the EU, apart from the US. The EU is five times more important to the Russian economy than vice-versa[232] and European countries have a closer trade relationship with Russia than the US does, so Russia could try to take advantage of the "increasing tensions between the United States and its allies and trading partners around the world," caused as "American sanctions have expanded and proliferated over the past 20 years,"[233] particularly unilaterally and with seemingly little care for the second- and third-order consequences for US allies. To that end, Russia has been running its own information operations among the European public, proliferating the idea that "measures are being imposed at the behest of and for the benefit of America, and against the interests of Europeans"[234] and suggesting that "the US created the crisis in Ukraine and then forced Europe into imposing restrictions."[235]

In addition to levying its own countersanctions against the US and other Western countries,[236] Russia has worked proactively to help its own economy by cultivating its relationships with African countries, both for the arms sales and for the diplomatic support in the UN.[237] The economic ties Russia is building with China are even more significant, from building "next generation heavy-lift helicopters" to AliExpress Russia –

Alibaba's partnership with Russia's Mail.ru and Megafon – to "plans to engage in the construction of a jointly produced Russian-Chinese CR929 long-haul, wide-body commercial aircraft" to Bank of China's $2 billion-dollar loan to Gazprom.[238] "The extent to which Russia can successfully execute a "pivot to China" . . . should not be overstated,"[239] however, and economic pledges are so tenuous that when AliExpress stopped filling orders originating from Crimea to avoid secondary sanctions from the US, the Russian press barely reported it[240] and Russia could hardly afford to substantively respond. China wields its great economic might in its trade with Russia the way it does with other weaker economies, namely, in a way that is advantageous for China. Russia-China trade is reportedly valued at $108 billion,[241] with China accounting for "some 90% of total cross-border shipments to Russia", and this trade imbalance likely constrains Russian action.[242]

The Future of US and EU Sanctions Against Russia

The West has several options for how to proceed with sanctions against Russia: (1) leave them in place and hope they work over time, (2) lift the sanctions and go back to business as usual, (3) keep the same objectives and change the sanctions, (4) keep the sanctions but adjust the objectives, (5) adjust both the sanctions and the objectives.[243] The sanctions regarding Ukraine have requirements to be met for lifting them, but one of Russia's critical vulnerabilities is that its leadership is more concerned with staying in power than with the country's economic development, so Russia's responses to the current sanctions have not been in its apparent economic best interest, and "there are open disagreements between EU member-states over the value and impact of sanctions,"[244] and how to proceed. It would be beneficial for some European countries to

normalize trade relations with Russia, and "a successful charm offensive by Russia, or effective coercion, might be enough to get a small number of member-states to block renewal of sanctions,"[245] or just turn a blind eye to sanctions busting, "since implementation is a national rather than an EU responsibility."[246] In March 2019 Italian Prime Minister Giuseppe Conte explicitly stated Rome's intent to work towards ending sanctions against Russia, calling them ineffective and harmful to the Italian economy.[247]

While changing the objectives may seem like moving the goalposts, one could also argue a readjustment just acknowledges the ground truth while keeping the situation from getting any worse. For Ukraine, a solid resistance effort supported by EU solidarity "has proved to be the most efficient way to stop Russian military advances"[248] – an important goal for Ukraine and something the EU can call a win. The longer the stalemate with Russia continues, the deeper the division between the US and the EU regarding how to change Russia's behavior. Meanwhile, EU participation is "critical to making sanctions bite,"[249] because the EU has significantly more economic leverage with Russia than the US, doing 12 times more trade with Russia than the US does.[250]

EU countries have their own exposure regarding trade with Russia, especially in the energy sector: in 2015 the EU overall imported nearly one third of its oil and gas from Russia,[251] with gas and nuclear sectors more vulnerable than the oil sector.[252] EU countries have been working to extricate themselves from Russia's energy grip, however, focusing especially on weaning itself off Russian gas.[253] European financial institutions also have exposure regarding sanctions against Russia's financial sector, having lent significant sums to Russian banks, so it is not in the EU's interest to let the Russian

economy completely tank because they have no desire to see Russian banks default on their loans.[254]

The future of joint US-EU sanctions against Russia seems tenuous at best, particularly given the level of concern regarding the health of their overall relationship and "broader European concerns about whether the [Trump] Administration regards the EU as a partner or a competitor."[255] If the US decides to maintain current objectives while ratcheting sanctions down further, it could work if the sanctions are "comprehensive and multilateral."[256] The key question in pursuing future sanctions, even if "imposing tougher sanctions is . . . likely to degrade the Russian economy, and could do so to a greater extent and more quickly than maintaining low oil prices,"[257] is: will they bring Russian behavior into compliance and prescribed by the US?

A Non-Sanctions-Based Economic Approach

Aside from the ability cryptocurrencies provide to enthusiasts for bucking the system, cryptocurrencies are attractive thanks to their lack of regulation, so international regulations could potentially make cryptocurrencies less disruptive.[258] Cryptocurrencies remain legally ambiguous in most countries because "private electronic money" challenges the very definition of money, making it difficult to determine if it constitutes legal tender, and not surprisingly, "the vast literature emanating from Central Bank projects throughout 2018 shows . . . they tend to provide a negative view on cryptocurrencies."[259] CB RF is also "clearly against [private digital currencies]" and a G7 report also concluded that cryptocurrencies are "a systemic risk."[260] The European CB went so far as to call cryptocurrencies "the evil spawn of the financial crisis," and published a study identifying "a large hypothetical scope for anticompetitive

behaviours."[261] The general regulatory attitude towards cryptocurrencies is that they are vulnerable to criminal use,[262] but if CBs decide to regulate them, they will likely identify them as a financial instrument other than money, and they will have to establish a significant multinational consensus, otherwise individual governments will fear they are creating unfair opportunities for countries who declare cryptocurrencies legal for unregulated use.

Cases of Creating a National Cryptocurrency

Benefits to Creating a National Cryptocurrency

The still new feel of cryptocurrencies and lack of international agreement on how to regard them – legal/illegal, money/not money, taxable/not taxable, something more like stocks and bonds – is what makes them attractive to nation-states with unstable economies, characterized by political paranoia. In examining three countries in the nascent stages of launching native cryptocurrencies, Venezuela, Iran, and Russia, Mahdavieh identifies several common factors affecting their economic strategy (see table 1). Overall, (1) kleptocratic regimes are more prone to adopt cryptocurrencies and (2) operating under Western sanctions also makes cryptocurrency adoption more likely; and, in relation to other countries, (3) a high level of corruption, (4) a low GDP, (5) a high level of economic volatility all contribute to embracing the idea of a national cryptocurrency.[263]

Table 1. Key Factors Contributing to Creating a National Cryptocurrency		
Attributes	**Definition**	**Measurement**
Kleptocracy	Corrupt form of government that "rules by theft"	Economic Freedom, Human Freedom Index, Corruption Perception Index
Corruption	Misuse of power to fulfill individualistic goals to acquire greater power	Corruption Perception Index
Resource-rich capabilities	Based on oil/natural gas	CIA Factbook
GDP	Total value of goods produced annually	World Bank
Economic Volatility	Vulnerability to international fluctuations possibly due to lack of economic diversification	Export revenue exceeding 50% classified as economically dependent, measuring depreciation of currency, and inflation
Western sanctions	United States and European Union imposing economic sanctions: penalties imposed on economy to produce desired outcome	U.S. and EU sanctions on case study countries

Source: Rose Mahdavieh, "'Governments' Adoption of Native Cryptocurrency: A Case Study of Iran, Russia, and Venezuela" (Honors Undergraduate Thesis, University of Central Florida, Orlando, FL, 2019), https://stars.library.ucf.edu/honorstheses/502, 18.

Cryptocurrency is attractive to governments that "feel constrained or short changed by established, traditional currency markets and mechanisms"[264] because they facilitate rapid transactions and their newness and lack of regulation means these countries may be able to get away with conduct and purchases they might not be allowed to otherwise. Cryptocurrencies provide a satisfying solution for these governments specifically because they challenge the hegemony of the almighty USD[265] and DLT has already had a global economic impact and in some countries has even affected political realities.[266]

Sanctions intensify the downward spiral of an already weak economy, so "kleptocratic regimes are coerced into finding an alternative solution to ensure their surviving reign,"[267] because one of the critical vulnerabilities of kleptocratic regimes is

their leaders' anxiety about and need to stay in power. The creation of a native cryptocurrency is not a straight line to circumventing sanctions, nevertheless, a country building more than one cryptocurrency evasion capability indicates a certain intent. In addition to using a national cryptocurrency to make purchases using a currency other than USD, governments can (1) use "state-controlled cyber activities" to "steal digital currencies" via hacking, (2) use their access to cheap electricity to mine traditional cryptocurrencies themselves, then use them for surreptitious purchases, or (3) work on creating a supracurrency with other countries to conduct trade while bypassing the USD.[268] While Venezuela has launched "the first native cryptocurrency backed by petroleum," North Korea has reportedly hacked existing cryptocurrency accounts,[269] a US Justice Department indictment stated Russian operatives "created Bitcoins themselves through the process known as mining,"[270] and BRICS has announced plans to launch its own BRICSCoin.[271]

Another critical vulnerability these countries share is a resources-rich but non-diversified economy, and particularly in Russia and Venezuela, this has left them vulnerable to 'Dutch Disease', an economic phenomenon in which the main export resource gets overly advantaged, while other exports get disadvantaged,[272] which has led to an even more specialized economy, leaving it even more vulnerable and undermining kleptocrats' source of power. This creates an environment in which "the intent for cryptocurrency culminates in efforts to expand power and exploitation."[273] In addition to circumventing sanctions, kleptocrats can use DLT "can easily enhance corruption in every socioeconomic sector,"[274] especially when the private encryption is not decentralized, yet is "only accessible to the government (and invited authorities)," those

with access could both launder money and embezzle or even steal. In this way, native cryptocurrencies "enhance corruption and allow kleptocracies to continue expanding power" and "push personal agendas."[275]

Venezuela's Petro

In early 2018, President Maduro of Venezuela explained the motivation for launching the Petro cryptocurrency to help the country "advance in issues of monetary sovereignty, to make financial transactions and overcome the financial blockade."[276] The Petro is backed by its namesake and its value is pegged to the price of oil, and is intended to function like a traditional cryptocurrency, to be traded on a cryptocurrency exchange.[277] The Venezuelan economy was ripe for a cryptocurrency launch, after being "plagued by a series of poor economic choices," resulting in hyperinflation of the bolivar, "with an inflation rate expected to reach over 3400 percent in 2019."[278] Economist Robert Looney puts the true motivation squarely in the money laundering camp: "The Petro's primary function would be to secretly move cash out of a collapsing economy and convert it into foreign currency," meant to benefit government insiders and their cronies,"[279] and several countries have already pointed out the potential for the government to use it "raise capital and skirt international sanctions."[280] One day after launching the Petro, Maduro announced the launch of Petro Gold, backed by the nation's gold reserves,[281] providing yet another opportunity for sidestepping sanctions, namely, by "forcing other countries to buy into or exchange for the sanctioned state cryptocurrency to purchase the given resource,"[282] at which point they could also manipulate prices and undercut the market.

As sector sanctions have taken their toll on Venezuela's and Russia's non-diversified economies, their level of outside economic investment and financial freedom have gone down,[283] and their shared motivation led to "a joint experiment between Russia and Venezuela to design and test a virtual currency in a sanctioned country."[284] Venezuela was a natural choice for Russia to use as a Petri dish, as "the partner that has most permitted Russia to use its territory and resources to advance Russian strategic objectives."[285] Russia leveraged its foreign military sales[286] and substantial financial support to its Latin American partner to avoid any economic and political crypto-backlash domestically while Venezuela "run the experiment on itself."[287] It supported the Venezuelan Petro from afar with technology, political, and financial backing standpoint, buying itself the ability to observe a live national currency operate in a fellow sanctioned country.

After raising a reported 735 million USD at its initial coin offering in 2018 and demonstrating "a state can develop and market a cryptocurrency internationally,[288] by 2019, the Petro appeared to have failed.[289] The US has already made Petro trading illegal for US citizens.[290] Evrofinance, a bi-national bank established to fund joint Russia-Venezuela oil and infrastructure projects, was the primary international financial institution backing the Petro.[291] In March 2019, OFAC designated the bank for sanctions; Russian state-backed Gazprombank and VTB Bank, each of which a 25% stakeholder in Evrofinance, had already been under sectoral sanctions since July 2014.[292]

Iran's Cryptorial

In November 2018, the SWIFT transfer system excluded certain Iranian banks,[293] at the behest of the US and by December the US Congress had already proposed the

Blocking Iran Illicit Finance Act, banning the Iranian national cryptocurrency and sanctioning those who would support its development.[294] When Iran's CB stated that its national cryptocurrency would be backed by its fiat currency, the rial,[295] the response was different from that in Russia, given the status of traditional cryptocurrencies in Iran at the time. Traditional cryptocurrencies are popular among Iranians and seem to some as "the only way to get money out of Iran," and cryptocurrency mining is both popular and, as of August 2019, legal.[296]

As in the cases of Venezuela and Russia, "countries that are still open to cooperating with Iran could easily explore avenues through the use of such sovereign coins,"[297] thus allowing Iran to circumvent sanctions. Iran's international trade situation, however, differs significantly from that of Russia and Venezuela: when only the US pulled out of the JCPOA, the remaining countries made a concerted effort to maintain their newly reestablished trade ties with Iran. In 2019, four of those countries were among the eight who conducted "negotiations on the use of cryptocurrencies in financial transactions" with Iran, and the same year, the EU launched Instex, a Special Purpose Vehicle to facilitate financial transactions with Iran.[298] In addition, Iran announced plans to sell its petroleum and "conduct international trade in currencies other than the US dollar,"[299] including an oil deal with China denominated in RMB. Corresponding banking is what makes it possible for "a financial institution in one country to do business in the currency of another,"[300] which has helped the Iranian financial institutions heavily sanctioned by the US.[301]

President Rouhani has defended Iran's national cryptocurrency as a way for the Muslim world to stand up to the "American financial regime" and its domination in

international trade, as well as to eliminate its reliance on the USD.[302] To that end, Iranian and Russian blockchain industries have agreed to cooperate in developing Iran's blockchain, "with a stated aim to address challenges arising from sanctions."[303] Iran's national cryptocurrency is one tool in its toolbox, which it can use together with traditional cryptocurrencies, non-dollar denominated trade deals, and other tools, to "challenge and subvert the U.S.-dominated financial architecture,"[304] thus elevating Iranian leadership's domestic standing and Iran's standing in the global economy.

While the cryptoruble differs from its analogs in that the Russian government (1) has not suggested it will be backed by a national resource or fiat currency, and (2) has not expressed an intent to trade it on the traditional cryptocurrency markets, it also shares significant features with its counterparts. All three cryptocurrencies are intended to be used to evade sanctions, challenge USD hegemony, and ultimately consolidate their nations' leaders' power. While all three are in their nascent stages, the implications for international sanctions and for US national security are significant.

---

[1] T. Macaulay, "How Governments around the World Are Using Blockchain," Computerworld, July 23, 2018, https://www.computerworlduk.com/galleries/applications/how-governments-are-using-blockchain-3680393/.

[2] "Head of MinComSvyazi RF Nikolay Nikiforov Has Found a Replacement for the Idea of a Cryptoruble," Smart-Lab, November 8, 2017, https://smart-lab.ru/tag.

[3] "Moiseev Suggests Using the Term 'Cyberruble' Instead of 'Cryptoruble'," *TASS*, November 15, 2017, http://tass.ru/ekonomika/4730204.

[4] Negodiay, "Can a State Cryptocurrency Compete With Bitcoin?" Tradernet, October 16, 2017, https://tradernet.com/feed/postId/1086632.

[5] Mahdavieh, "Governments' Adoption," 19.

[6] Robert W. Taylor, Eric J. Fritsch, John Liederbach, Michael R. Saylor, and William L. Tafoya, *Cyber Crime and Cyber Terrorism* (New York: Pearson, 2019), 370.

[7] Sokolova, "Crypto Way Around."

[8] Naumov, "Digital Sovereignty: Why The Government."

[9] "Putin Has Decided Russia Will Issue its Own Cryptocurrency," *Cryptorussia,* October 14, 2017, https://cryptorussia.ru/news/ putin-prinyal-reshenie-o-tom-chto-rossiya-vypustit-svoyu-kriptovalyutu.

[10] Yekaterina Smirnova and Yelena Mukhametshina, "FSB Helping Develop an International Blockchain Standard: This will allow Russian state bodies to use the new technology in the future," *Vedomosti*, August 18, 2017, https://www.vedomosti.ru/ technology/articles/2017/08/18/730045-fsb-blokcheina.

[11] David Hyland-Wood and Shahan Khatchadourian. "A Future History of International Blockchain Standards," *The Journal of The British Blockchain Association* 1 (June 2018): 3, https://www.researchgate.net/publication/326081291.

[12] "Masterchain Russian national blockchain network," *TAdvisor*, accessed March 15, 2020, http://tadviser.com/index.php/Product:Masterchain_Russian_national_ blockchain_network.

[13] Mahdavieh, "Governments' Adoption of Native Cryptocurrency," 34.

[14] Anna Baydakova, "'Disappointed' by Central Bank Blockchain, Russia's Largest Bank Eyes Alternatives," Yahoo Finance, July 2, 2019, https://finance.yahoo.com/news/russia-largest-bank-quitting-central-080038612.html.

[15] Ibid.

[16] U.S. Congress, Senate, "Statement of General Paul M. Nakasone Commander U.S. Cyber Command before the Senate Committee on Armed Services," February 14, 2019, 4, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.

[17] Russian President, "President's Address"

[18] "MinComSvyazi: We Need Digital Sovereignty to Develop the Economy," *RIA Novosti,* September 5, 2017, https://ria.ru/soceity/20170905/1501809181.html.

[19] Balakirev.ia, "The Authorities Offer A Cryptoruble," *Vedomosti,* October 18, 2017, https://www.vedomosti.ru/comments/economics/articles/2017/10/18/738302-vlasti-predloshit-kriptorubl#/.

[20] A. Baulin, "Will Blockchain Online Become The Distribution Register for a New Economic Idea?" October 31, 2017, http://www.forbes.ru/tehnologii/351861-blokcheyn-v-efire-stanet-li-raspredelennyy-reestr-novoy-ekonomicheskoy-ideey.

[21] "FT: Russia Is Looking For A Way."

[22] Smirnova and Mukhametshina, "FSB Helping."

[23] "Masterchain."

[24] "Bank of Russia and Market Participants Have Developed Masterchain Prototype and Successfully Made First Test Transactions," Bank of Russia, October 5, 2016, https://www.cbr.ru/eng/press/event/?id=643.

[25] Baydakova, "'Disappointed.'"

[26] "Masterchain."

[27] Welt et al., *U.S. Sanctions on Russia*, 15.

[28] Office of the Director of National Intelligence (DNI), *Global Trends: Paradox of Progress* (Washington, DC: National Intelligence Council, 2017), www.dni.gov/nic/globaltrends.

[29] Frebowitz, "Cryptocurrency and State Sovereignty," 69.

[30] Megan Taylor, "Russia Picks Prime Bitcoin Mining Territory as CryptoRuble Launch Nears," *Bitsonline*, November 18, 2017, https://bitsonline.com/russia-bitcoin-mining-cryptoruble/.

[31] U.S. Congress, Senate, "Foreign Cyber Threats to the United States," Joint Statement for the Record to the Senate Armed Services Committee by The Honorable James R. Clapper, Director of National Intelligence; The Honorable Marcel Lettre, Undersecretary of Defense for Intelligence; and Admiral Michael S. Rogers, Commander U.S. Cyber Command, Director National Intelligence Agency; January 2017.

[32] Ibid.

[33] Ibid.

[34] Taylor et al., *Cyber Crime*, 370.

[35] JCS, JOE 2035.

[36] "FT: Russia Is Looking For A Way."

[37] "Sergey Glazyev."

[38] "An unusual Way."

[39] "Cryptocurrencies: The Ideal Way to Get around Sanctions," *Teknoblog* (blog), December 18, 2017, https://teknoblog.ru/2017/12/18/85669.

[40] Howard J. Shatz, *US International Economic Strategy in a Turbulent World* (Santa Monica, CA: RAND Corporation, 2016), 121.

[41] Ibid.

[42] Frebowitz, "Cryptocurrency and State Sovereignty," 9.

[43] Mahdavieh, "Governments' Adoption," 34.

[44] Ibid., 36.

[45] Ibid.

[46] Kakushadze and Liew, "CryptoRuble: From Russia," 3.

[47] Ibid.

[48] Cyrus Newlin, "U.S. Sanctions against Russia: What You Need to Know," Center for Strategic and International Studies, October 31, 2018. https://www.csis.org/analysis/us-sanctions-against-russia-what-you-need-know.

[49] Ibid.

[50] U.S. Congress. Senate. "Statement of General Paul M. Nakasone," 5.

[51] Ibid., 2.

[52] TRADOC, TRADOC Pamphlet 525-3-1, A-1.

[53] Ibid., GL-2.

[54] Ibid., 26.

[55] Jim Garamone, "European Command Exercise Program Aims to Deter Russia," U.S. Department of Defense, June 3, 2019, https://www.defense.gov/explore/story/Article/1864862/european-command-exercise-program-aims-to-deter-russia/.

[56] TRADOC, TRADOC Pamphlet 525-3-1, vi.

[57] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, no. 92 (1st Quarter 2019): 10-14, 11.

[58] Ibid.

[59] TRADOC, TRADOC Pamphlet 525-3-1, 7.

[60] JCS, JOE 2035.

[61] Pynnöniemi, "Russia's National Security Strategy"

[62] Georgiy Pocheptsov, "How Influence Operations, Mass Culture, and Social Media Construct a New Reality," Noravank, May 8, 2018, www.noravank.am/rus/articles/detail.php?ELEMENT_ID=16944&print=Y.

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] TRADOC, TRADOC Pamphlet 525-3-1, iii.

[67] Frebowitz, "Cryptocurrency and State Sovereignty," 9.

[68] TRADOC, TRADOC Pamphlet 525-3-1, 6.

[69] IISS, "War, power, rules."

[70] Taylor et al., *Cyber Crime*, 3-4.

[71] Office of the Director of National Intelligence (DNI), *National Intelligence Strategy of the United States of America* (Washington, DC: DNI, 2019), 4.

[72] U.S. President, NSS, 34.

[73] DNI, *National Intelligence Strategy*, 4.

[74] U.S. Congress, Senate, "Worldwide Threat Assessment," Statement for the Record by James R. Clapper, Director of National Intelligence, *Hearing before the Select Committee on Intelligence,* 113th Cong., 1st sess., March 12, 2013, 8.

[75] TRADOC, TRADOC Pamphlet 525-3-1, 6.

[76] Ibid., vi.

[77] Taylor et al., *Cyber Crime*, 43.

[78] Ibid., 405.

[79] Ibid.

[80] U.S. Congress, Senate, "Worldwide Threat Assessment," 2.

[81] U.S. Congress, Senate, "Foreign Cyber Threats to the United States."

[82] U.S. Department of Defense (DOD), *Summary: Department of Defense Cyber Strategy* (Washington, DC: DOD, 2018), 4.

[83] TRADOC, TRADOC Pamphlet 525-3-1, iii.

[84] U.S. Department of Defense, Chief Information Office (DOD CIO), Department of Defense Instruction (DODI) No. 8500.01, Incorporating Change 1, Subject: Cybersecurity, Washington, DC, October 7, 2019, 2.

[85] TRADOC, TRADOC Pamphlet 525-3-1, x.

[86] Ibid., 24.

[87] U.S. Congress, Senate, "Statement of General Paul M. Nakasone," 2.

[88] Ibid., 9-10.

[89] Mark Pomerleau, "Is there such a concept as 'cyber deterrence'?" *FifthDomain,* April 30, 2019. https://www.fifthdomain.com/dod/2019/04/30/is-there-such-a-concept-as-cyber-deterrence/.

[90] DOD, *Summary: Department of Defense Cyber Strategy*, 2.

[91] Taylor et al., *Cyber Crime*, 50.

[92] Gary R. Gordon, Chet D. Hosmer, Christine Siedsma, Don Rebovich, "Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime" (Research Report, Document No. 198421, Study sponsored by the National Institute of Justice, February 4, 2002), 3.

[93] Richard Berkebile, "Thoughts on Force Protection," *Joint Forces Quarterly* 81 (2nd Quarter 2016): 145.

[94] U.S. Congress, Senate, "Worldwide Threat Assessment," 7.

[95] TRADOC, TRADOC Pamphlet 525-3-1, 27.

[96] U.S. Congress, Senate, "Statement of General Paul M. Nakasone," 3.

[97] Nakasone, "A Cyber Force for Persistent Operations," 12.

[98] U.S. Congress, Senate, "Statement of General Paul M. Nakasone," 6.

[99] Theresa Hitchens, "US Urges 'Like-Minded' Countries To Collaborate On Cyber Deterrence," *Breaking Defense*, April 24, 2019, 13, https://breakingdefense.com/2019/04/us-urging-likeminded-countries-to-collaborate-on-cyber-deterrence/.

[100] Ibid., 15.

[101] Ibid., 14.

[102] Frebowitz, "Cryptocurrency and State Sovereignty", 9.

[103] TRADOC, TRADOC Pamphlet 525-3-1, 31.

[104] Jeff Kosseff, "The Contours of 'Defend Forward' Under International Law," 11th International Conference on Cyber Conflict: Silent Battle, eds. T. Minarik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky (Tallinn: NATO CCD COE Publications, 2019), 3.

[105] U.S. Congress, Senate, "Worldwide Threat Assessment," 2.

[106] U.S. Army Training and Doctrine Command (TRADOC) and U.S. Army Futures Command, "Potential Game Changers through 2050 (The Era of Contested Equality)," Broadsheet, July 25, 2019, 3.

[107] Pomerleau, "Is There Such a Concept."

[108] Kosseff, "The Contours of 'Defend Forward," 5.

[109] Ibid.

[110] Ibid., 11.

[111] Pomerleau, "Is There Such a Concept"

[112] U.S. Congress, Senate, "Worldwide Threat Assessment," 4.

[113] Headquarters, Department of the Army (HQDA), Army Regulation (AR) 25-2, *Information Management: Army Cybersecurity* (Washington, DC: Government Publishing Office, April 4, 2019), 11.

[114] Ibid., 12.

[115] Kosseff, "The Contours of 'Defend Forward'," 1.

[116] U.S. President, NSS.

[117] Ibid., 34.

[118] Ibid.

[119] Ibid., 3.

[120] Ibid., 31

[121] Ibid., 32.

[122] Ibid., 34.

[123] DNI, *National Intelligence Strategy* 1.

[124] Ibid., 5.

[125] Ibid.

[126] U.S. President, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 1.

[127] Ibid., 2.

[128] Ibid., 3.

[129] Ibid., 4.

[130] Ibid., 5.

[131] Ibid., 6.

[132] Ibid., 21.

[133] Ibid., 15.

[134] Ibid., 20.

[135] Ibid., 21.

[136] Ibid.

[137] Ibid., 26.

[138] Ibid., 21.

[139] TRADOC, TRADOC Pamphlet 525-3-1, 24.

[140] DOD, *Summary: Department of Defense Cyber Strategy*, 2018, 1.

[141] Ibid., 7.

[142] Ibid., 1.

[143] Ibid., 4.

[144] Ibid., 7.

[145] Bond et al., "Frozen," 4.

[146] Shatz, *US International Economic Strategy*, 120.

[147] Welt et al., *U.S. Sanctions on Russia*, 4.

[148] Ibid.

[149] Mahdavieh, "Governments' Adoption," 5.

[150] Ibid.

[151] Ibid., 6.

[152] Ibid.

[153] Ibid.

[154] U.S. Department of the Treasury, "Economic Policy," https://home.treasury.gov/policy-issues/economic-policy.

[155] U.S. Department of the Treasury, "Office of Foreign Assets Control – Sanctions, Programs, and Information," https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

[156] Welt et al., *US Sanctions Against Russia*, 5.

[157] Financial Crimes Enforcement Network, U.S. Treasury, "Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium," New York, NY, November 15, 2019, https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-chainalysis-blockchain-symposium.

[158] Ibid.

[159] Ibid.

[160] Welt et al., *U.S. Sanctions on Russia*, 1.

[161] Ibid.

[162] Ibid., 2.

[163] Newlin, "U.S. Sanctions against Russia."

[164] Welt et al., *U.S. Sanctions on Russia*, 7.

[165] Ibid., 1

[166] U.S. Department Office of Foreign Assets Control, "Ukraine/Russia-Related Sanctions Program," last updated June 16, 2016, 1.

[167] Ibid., 4.

[168] Newlin, "U.S. Sanctions against Russia".

[169] Welt et al., *U.S. Sanctions on Russia*, 3.

[170] Ivan Gutterman, Wojtek Grojec, and RFE/RL's Current Time, "A Timeline Of All Russia-Related Sanctions. A detailed look at all the sanctions levied against Russia, and its countersanctions, since 2014," *Radio Free Europe Radio Liberty,* September 19, 2018, https://www.rferl.org/a/russia-sa.

[171] Welt et al., *U.S. Sanctions on Russia*, 21.

[172] Gutterman, Grojec, and RFE/RL's Current Time, "A Timeline."

[173] Welt et al., *U.S. Sanctions on Russia*, 2.

[174] Ibid., 11.

[175] Newlin, "U.S. Sanctions against Russia."

[176] Ibid.

[177] Welt et al., *U.S. Sanctions on Russia*, 2.

[178] Bond et al., "Frozen," 1.

[179] Dianne E. Rennack and Cory Welt, "U.S. Sanctions on Russia: An Overview," *In Focus*, Congressional Research Service, January 2, 2019. www.crs.gov.

[180] Shatz, *US International Economic Strategy*, 122.

[181] Bryan R. Early and Keith Preble, "'Sanctions Busting': The Risks and Rewards to those Trying to Circumvent the System," SanctionsAlert.com, June 15, 2018. https://sanctionsalert.com/sanctions-busting-the-risks-and-rewards-to-those-trying-to-circumvent-the-system/.

[182] Ibid.

[183] Ibid.

[184] Ibid.

[185] Cullen S. Hendrix, "Freezing Iran Out of Oil Markets Won't Work," *Denver Post*, August 13, 2018, https://www.piie.com/commentary/op-eds/freezing-iran-out-oil-markets-wont-work.

[186] Bond et al., "Frozen," 19.

[187] Shatz, *US International Economic Strategy*, 122.

[188] Ibid.

[189] Mahdavieh, "Governments' Adoption," 3.

[190] Shatz, *US International Economic Strategy*, 122.

[191] Hendrix, "Freezing Iran Out."

[192] Chen Aizhu, Shu Zhang, Florence Tan, Muyu Xu, Timothy Gardner, Jeff Mason, and Parisa Hafezi, "China continued Iran oil imports in July in teeth of U.S. sanctions: analysts," *Reuters*, August 8, 2019, https://www.reuters.com/article/us-china-iran-oil/china-continued-iran-oil-imports-in-july-in-teeth-of-u-s-sanctions-analysts-idUSKCN1UY11S.

[193] David Pan, "Iran President: We Need a Muslim Cryptocurrency to Fight the US Dollar," *Coindesk*, December 19, 2019, https://www.coindesk.com/iran-president-we-need-a-muslim-cryptocurrency-to-fight-the-us-dollar.

[194] Kimberley Ann Elliott, "Evidence on the Costs and Benefits of Economic Sanctions," Speech given before the Subcommittee on Trade, Committee on Ways and Means, United States House of Representatives Washington, DC, October 23, 1997.

[195] Ibid.

[196] Welt et al., *U.S. Sanctions on Russia*, 2.

[197] Elliot, "Evidence."

[198] Michael Greenwald, "Russia and China Are Hard Targets for U.S. Sanctions. That Could Be a Problem," *Barron's*, February 29, 2020, https://www.barrons.com/articles/russia-and-china-are-hard-targets-for-u-s-sanctions-that-could-be-a-problem-51582986656.

[199] Shatz, *US International Economic Strategy*, 123.

[200] Bond et al., "Frozen," 18.

[201] Greenwald, "Russia and China."

[202] Newlin, "U.S. Sanctions against Russia."

[203] Ibid.

[204] Ibid.

[205] Welt et al., *U.S. Sanctions on Russia*, 3.

[206] Ibid.

[207] Ibid.

[208] Ibid., 46.

[209] Ibid., 47.

[210] Ibid.

[211] Dobins, "Nonviolent Ways."

[212] Bond et al., "Frozen," 20.

[213] Newlin, "U.S. Sanctions against Russia".

[214] Mahdavieh, "Governments' Adoption," 34.

[215] Bond et al., "Frozen," 9.

[216] Ibid.

[217] Ibid.

[218] Welt et al., *U.S. Sanctions on Russia*, 1.

[219] Heather Conley, "Drivers and Ramifications of US Sanctions Policy Towards Russia," SMA General Speaker Series, Center for Strategic and International Studies, 10 October 2019, https://nsiteam.com/drivers-and-ramifications-of-us-sanctions-policy-towards-russia/.

[220] Welt et al., *U.S. Sanctions on Russia*, 3.

[221] Bond et al., "Frozen," 6.

[222] Ibid., 7.

[223] Welt et al., *U.S. Sanctions on Russia*, 44.

[224] Ibid., 3.

[225] Ibid., 1.

[226] Ibid., 41.

[227] Ibid., 48.

[228] Ibid.

[229] Ibid.

[230] Conley, "Drivers and Ramifications."

[231] Welt et al., *U.S. Sanctions on Russia*, 44.

[232] Bond et al., "Frozen," 5.

[233] Elliot, "Evidence."

[234] Bond et al., "Frozen," 4.

[235] Ibid., 17

[236] Welt et al., *U.S. Sanctions on Russia*, 32.

[237] Malin Severin, "Russian Activities in Africa (Continued)," in *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper,* ed. Nicole Peterson (Washington, DC: Department of Defense, Joint Chiefs of Staff, Freedom's Fortress, May 2019), 72.

[238] Welt et al., *U.S. Sanctions on Russia*, 48.

[239] Ibid.

[240] RWR Advisory Group LLC, "Monthly Report on Developments in the Economic and Financial Threat Domain, EAST ASIA August 2019: Assessing the Soft Power Projection Strategies of Key Russian State-Controlled Enterprises and Other Transactional Components of the Economic and Financial Threat Domain," (prepared for United States European Command's Russia Strategic Initiative, September 3, 2019), 3.

[241] Ibid., 7.

[242] Ibid., 15.

[243] Bond et al., "Frozen," 17.

[244] Ibid., 16.

[245] Ibid.

[246] Ibid., 17.

[247] Gavin Jones, "Italy PM says is working to try to end sanctions against Russia," *Reuters,* March 8, 2019, www.reuters.com.

[248] Liubov Nepop, "Is it time for Europe to excuse Russia's aggression?" *Euractiv*, September 25, 2015. www.euractiv.com.

[249] Newlin, "U.S. Sanctions against Russia."

[250] Bond et al., "Frozen," 4.

[251] Ibid.

[252] Ibid., 15.

[253] Ibid.

[254] Ibid., 16.

[255] Welt et al., *U.S. Sanctions on Russia*, 39.

[256] Dobbins et al., *Overextending and Unbalancing Russia*, 3.

[257] Dobbins, "Nonviolent Ways."

[258] Frebowitz, "Cryptocurrency and State Sovereignty," 93.

[259] Ward and Rochemont, "Understanding Central Bank," 1.

[260] Miranda Wood, "Russia to confiscate crypto, central bank against private digital currency," *Ledger Insights,* November 8, 2019, https://www.ledgerinsights.com/russia-confiscate-crypto-private-digital-currency/.

[261] Ward and Rochemont, "Understanding Central Bank," 20.

[262] Ibid.

[263] Mahdavieh, "Governments' Adoption," ii.

[264] Ibid., 1.

[265] Ibid.

[266] Ibid., 2.

[267] Ibid., 12.

[268] Ibid.

[269] Daniel Palmer, "North Korea Stole $2 Billion in Crypto and Fiat to Fund Weapons Programs," *Coindesk*, August 6, 2019, https://www.coindesk.com/north-korea-stole-2-billion-in-crypto-and-fiat-to-fund-weapons-programs.

[270] Nathaniel Popper and Matthew Rosenberg, "How Russian Spies Hid behind Bitcoin in Hacking Campaign," *New York Times,* July 13, 2018, https://www.nytimes.com/2018/07/13/technology/bitcoin-russian-hacking.html.

[271] Mahdavieh, "Governments' Adoption," 12.

[272] Bond et al., "Frozen," 6.

[273] Mahdavieh, "Governments' Adoption," 60.

[274] Ibid.

[275] Ibid., 7.

[276] Tsvetana Paraskova, 2017, "Venezuela to Launch Oil-Backed Petro Cryptocurrency within Days," OilPrice.com, December 29, 2017, https://oilprice.com/Energy/Crude-Oil/Venezuela-To-Launch-Oil-Backed-Petro-Cryptocurrency-Within-Days.html.

[277] Frebowitz, "Cryptocurrency and State Sovereignty," 73.

[278] Ibid., 74.

[279] Ibid.

[280] Ibid.

[281] Ibid., 75.

[282] Ibid., 91.

[283] Mahdavieh, "Governments' Adoption," 10.

[284] Frebowitz, "Cryptocurrency and State Sovereignty," 74.

[285] R. Evan Ellis, "Russian Activities in Latin America," in *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper,* ed. Nicole Peterson (Washington, DC: Department of Defense, Joint Chiefs of Staff, Freedom's Fortress, May 2019), 78.

[286] Michael Zennie, "Here's Why Russian Bombers Are in Venezuela. And Why the U.S. Is So Angry about It," *MSN*, http://www.msn.com/en-us/news/world/heres-why-russian-bombers-are-in-venezuela-and-why-the-us-is-so-angry-about-it/ar-BBQV0FI?ocid=ientp, December 14, 2018.

[287] Frebowitz, "Cryptocurrency and State Sovereignty," 75.

[288] Ibid.

[289] U.S. Department of the Treasury. "Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela." Press Release. March 11, 2019. https://home.treasury.gov/news/press-releases/sm622.

[290] Frebowitz, "Cryptocurrency and State Sovereignty," 74.

[291] Ibid.

[292] Ibid.

[293] "US Excludes Iran's Central Bank from the Global Financial System," Bitcoin, November 8, 2018, https://news.bitcoin.com/us-excludes-irans-central-bank-from-the-global-financial-system/.

[294] Mahdavieh, "Governments' Adoption," 59.

[295] Ratna, "Iran Has a Bitcoin Strategy."

[296] Ibid.

[297] Ibid.

[298] Ibid.

[299] "How does Iran plan to get around US sanctions? Use other currencies," *The Washington Post*, September 30, 2018.

[300] Greenwald, "Russia and China Are Hard Targets."

[301] Pan, "Iran President."

[302] Ibid.

[303] Ratna, "Iran Has a Bitcoin Strategy."

[304] Ibid.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

According to the US National Intelligence Strategy, "our adversaries are becoming more adept at using cyberspace capabilities to threaten our interests and advance their own strategic and economic objectives,"[1] and Russia appears intent on using the cryptoruble as a cyber tool to do just that. The Digital Economy as not only a national economic program, but a way to establish "digital sovereignty" in a world lived much of the time in cyberspace. Native cryptocurrencies are still nascent in both their development and use, and US policy is also just starting to respond. The US took early steps to block them using sanctions against trading in Venezuelan and Iranian cryptocurrencies, and the question now is what proactive steps the US will take regarding cryptoruble and if it will apply a more comprehensive approach than sanctions alone. Once Russia can conduct cryptoruble transactions with actors outside the country, the administration may be able to buy more than just the energy technologies they have been denied for years. It is unclear what they will buy or which efforts (state or non-state) they will fund, however, the potential for realizing a gray-zone threat to US national security is clear.

Sanctions are necessary but not sufficient to deter Russia's malign behavior. In the last decade, US and combined US-EU sanctions have contributed to Russia's economic decline. As Bond et al. suggest, "Russia's economy is in a mess, not primarily because of the sanctions, but as a result of a falling oil price, a falling rouble and Russia's own economic policy mistakes. Sanctions reinforce the effects of other problems."[2] While oil and gas prices run their course, circumventing sanctions would at least allow

the Russian administration to "alleviate some of the pressure on the main sectors of the economy, and especially on the oligarchs being squeezed."[3] Given the dominance of the dollar in transnational transactions worldwide, and given its status as the de facto world currency, comprising "up 64 percent of all known central bank foreign exchange reserves,"[4] Russia has a vested interest in finding a way to bank, buy, and trade without having to use the ubiquitous USD.

In answering the research question, "What are the ramifications of a Russian cryptoruble for US national security?" three main points become apparent: (1) Russia will likely try to use it to circumvent sanctions, which could threaten US security by allowing the Russian government to refill its coffers and/or by allowing Russia to get its hands on dangerous technology, weapons, or materiel; (2) cryptoruble's traceability could afford US security organizations the advantage in access and surveillance; (3) the executive branch could shore up the legal justification for tracing efforts by establishing policy and strategy focusing on the nexus of economic and national security threats and safety.

Implications for Practice

If the US is not proactive in addressing the threat of cryptoruble and Russia is able to find trading partners who will accept it as a form of payment, Russia could deny the international community the ability to carry out economic sanctions. If they can do that, they may be able to parlay that into their desired end state of a multipolar/regional power structure. If the world is indeed headed towards something other than a unipolar structure, in which no one country will be able to maintain hegemony by 2050, actors' power in the world will depend on alliances. If the US does not address this cyber capability in the near future, it will be dealing with cryptoruble sooner than it thinks.

As has been evident with the rise of the prominence of economic matters in global affairs, international economic issues are at the heart of global power shifts and Russia is one of the authoritarian regimes that regularly "blur[s] economic and political power."[5] Since 2016, the EU has expressed discomfort with the US levying unilateral sanctions, and has expressed an interest in finding ways to reengage with Russia. While trade with Russia is more significant for the EU than for the US, the latter has an enduring interest in protecting its allies and partners, in addition to itself, against any economic or security malfeasance the cryptoruble may portend.

The way forward with Russia will likely include a combination of statehood tools across DIME and require a whole-of-government approach as competition below-the-threshold increases. Although "Russia will bear the cost of this increased competition less easily than the United States will," for maximum effectiveness, the US must consider many different combinations and, given the risks involved, when it comes to Russia, "every option must be deliberately planned and carefully calibrated to achieve the desired effect."[6] Cyberspace operations are already being conducted below the level of armed conflict and US adversaries will continue to create new tools to operate it in it. Unlike traditional cryptocurrencies, Russian authorities have stated cryptoruble will be traceable because there is no need for anonymity. The official line is, if you are engaging in legal transactions, you have nothing to hide, and if you are engaging in illegal transactions, the government should have the right and ability to monitor and detect that. This is an opportunity for the US too: while cryptoruble purportedly uses a "buffer layer that only the Russian government has control over,"[7] it is built on the framework of the popular Ethereum cryptocurrency. The US could explore a combined bottom-up and top-down

approach, namely, working to track cryptoruble flows from a tactical standpoint, while establishing a National Economic Security Strategy, nested within the NSS, so the IC the proper authorities and guidance to use the tools it creates.

Confronting cryptoruble will likely take the US into contested space,[8] and the national security response would be to deny Russia freedom of action within that space outright or through tracking. The US may use overlapping tools to open windows of superiority[9] to prevent Russia from using cryptoruble or influence its would-be trading partners not to engage. If the US is to engage effectively on cryptoruble, it will need to both "challenge underlying assumptions" regarding the effectiveness of the current sanctions region, as well as "understand the capabilities and goals" of cryptoruble to "maximize deterrence."[10] EO sanctions that deny access to financial systems to states and individuals can put markets in that country at significant risk,[11] however, as Russia has shown, even a crippled economy does not force a country's leaders to change their behavior, cf. the still annexed Crimea and still occupied/contested Eastern Ukraine. One recommendation for further research from this thesis is to examine how to formulate future sanctions such that the requirements are more specific and the conditions for lifting sanctions are clearly stated. The question to explore is to what degree the sanctioned actor changes their behavior as dependent on the degree to which the actor believes the sanction is liftable and will be lifted once the conditions are met.

The Value of a National Economic Security Strategy

To reflect the national security implications of economic challenges at the next level of granularity, analogous to the National Defense Strategy (NDS) in relation to the NSS, the US could establish a National Economic Security Strategy (NESS), nested with

the NSS and fleshing out economic security requirements and actions in greater detail. Establishing the NESS as a document and necessitating a separate strategy-making process would address the nexus of security and economic threats, reflecting NSS 2017 Pillar II, "economic security is national security".[12] It would provide guidance by establishing strategic economic objectives, and nesting the NESS under the NSS, parallel to the NDS, would raise economy to the same level of importance as military in the DIME tool box of national power. One such proposal, as envisioned by Meyer and Sitaraman, would create a Department of Economic Growth and Security, which would join together five different economic functions, all in service of stated NSS goals, including addressing economic security issues that "arise from increased global economic inter-connectedness, particularly with countries like Russia and China."[13] An additional benefit may be the ability to recruit new talent into the federal government, as the NESS would highlight the importance of the field of national security responsibility.

If the NESS is to effectively guide economic security actions, civilian and military leaders should both be part of the strategy-making process, as their "responsibilities and interests overlap considerably."[14] While the Executive Branch has its own National Economic Council, the NEC's principle functions are purely economic[15] and "international economic policy is not usually at the center . . . of the foreign policy agenda"[16] nor of the national security agenda. Part of the challenge to forming and executing a national economic security strategy is the dispersed authority for trade policy among different parts of the executive branch.[17] The Obama administration proposed "merging the Department of Commerce, Small Business Administration, USTR, Ex-Im Bank, OPIC (Overseas Private Insurance Corporation, now known as the

US International Development Finance Corporation), and USTDA (US Trade and Development Agency),"[18] in recognition of the vital role both domestic and international policy play "in shaping and implementing the United States' grand strategy."[19] The 2012 proposal, however, "did not include a serious effort to unify economic security operations,"[20] and a singular office or strategy to address national economic security have yet to appear.

In recent years, the intersections of foreign economic policy and national security concerns have come into stark relief, given China's massive economic growth, military development, and territorial expansionism. Trade with Russia affects US national security indirectly but significantly, because the predominance of the USD as the currency of world trade makes escaping the USD-dominated system an attractive goal for Russia. When Russia launches its new weapon in this war on the Western financial system, cryptoruble, the US could be caught flat-footed if it does not have a coherent strategy in place for addressing the geostrategic and economic security consequences.

Jennifer Harris and Robert Blackwill "have argued for making 'geoeconomics' central to foreign policy, which appears to be reflected to some degree in the NSS, nevertheless, when the US Trade Representative tells the Senate Finance Committee he "[can]not speak to whether the Commerce Department had vetted its national security determinations through the National Security Council,"[21] that indicates a disconnect between economic strategy and national security strategy. As Russia becomes ever more economically intertwined with US allies, partners, and adversaries, the question of sanctions becomes more delicate. The US has little desire to impose secondary sanctions on allies who do business with sanctioned sectors – as it has shown by a failure to

activate such measures as required by CAATSA – and no desire to push Russia into the arms of those actors who can afford to disregard the threat of secondary sanctions. NESS would dedicate resources to addressing issues at the nexus of economic and national security and participants may have a voice in national policymaking as well. Cryptoruble could be the catalyst that "both spur[s] and legitimize[s] efforts inside and outside the government to think seriously"[22] about the cross-functional efforts needed to address it and other threats to both economic security and national security.

A Whole-of-Government Approach

The variety of tools in the statecraft toolbox was recognized before DIME became a convenient acronym to talk about them, however, the use of DIME as a common framework across the federal government recognizes the important contribution each area makes, with information and economy coming to prominence in recent years. Similarly, the concept of MDO recognizes not just the importance of a combined arms approach, but its importance across multiple domains and across the range of military operations including below the threshold of armed conflict and post-conflict. This spectrum applies not only to the military, and while not indicating a necessary linear transition from one step to the next, it does reflect the gradation present in current global interactions, i.e. it the elements of DIME can be applied together and actions in all four realms occur at different points along the spectrum. In the interest of protecting national security, the US approach to addressing cryptoruble should recognize, "In a global context, economic success and technological innovation, as well as military prowess, contribute to national power," and "these policy areas are inextricably bound together."[23]

As in other areas of national security, US success will depend on collaboration with other nations, along vectors of security cooperation, economic, and information influence. US national interests are global, "and because [its economic and geopolitical interests] are tied to its security interests, there is little choice but to engage globally."[24] With their recent adventurism, Russia and China in particular seem bent on disrupting or ignoring the rules-based international order, however, Shatz suggests the system is still useful, and the US "should strive to maintain and improve the system, integrating growing economic powers to maintain system legitimacy, improving global rules to foster free exchange . . . [so] countries find the US-led system a desirable one in which to participate."[25] While the US considers leading a world effort to regulate both traditional and native cryptocurrencies, it can also engage with allies and partners at the top level (policy and strategy) as well as the tactical level (cryptoruble tracing).

According to the National Cyber Strategy, in addition to cyber tools and strategy, the US "must also have policy choices to impose costs if it hopes to deter malicious cyber actors and prevent further escalation."[26] Strategy supports policy and "is an instrumental device that is given meaning by policy,"[27] so any voice at the policymaking table that keeps the intertwined nature of economic and national security in the discussion will support both economic and national security strategies. Authorities also give meaning to strategy, and just as MDO requires "establishing necessary authorities and permissions normally reserved for conflict . . . to operate in competition,"[28] addressing cryptoruble in the various threats it poses may require pushing authority down to more tactical levels, providing "access to and presence in . . . military and civilian networks,"[29] particularly as regards tracing currency flows.

The spectrum of global interaction provides guidance for next steps towards ensuring US national security. According to TRADOC, "The current conceptual framework [2018] of the Joint Force and the Army does not . . . acknowledge the need to compete below the threshold of armed conflict against a near-peer adversary to expand the competitive space for policymakers,"[30] yet organizations contributing to the national security effort could address threats in the sub-threshold zone if they had the terra firma of policy and strategy to stand on. The effective approaches to cryptoruble will be cross-functional and deterrence will likely require engagement in the competition space.

---

[1] DNI, *National Intelligence Strategy,* 11.

[2] Bond et al., "Frozen," 1.

[3] Ibid.

[4] Frebowitz, "Cryptocurrency and State Sovereignty," 80.

[5] Meyer and Sitaraman, "It's Economic Strategy."

[6] Dobbins et al., "Overextending and Unbalancing Russia," 12.

[7] Kakushadze and Liew, "Cryptoruble: From Russia," 3.

[8] TRADOC, TRADOC Pamphlet 525-3-1, GL-2.

[9] Ibid., GL-9.

[10] Ibid., i.

[11] Greenwald, "Russia and China Are Hard Targets."

[12] U.S. President, NSS, 17.

[13] Ibid.

[14] Chris Springer, "U.S. Military Professionals' Guide to Understanding Strategy," U.S. Army Command and General Staff College, Fort Leavenworth, KS.

[15] The White House, "White House National Economic Council," https://obamawhitehouse.archives.gov/administration/eop/nec.

[16] Meyer and Sitaraman, "It's Economic Strategy."

[17] Ibid.

[18] Ibid.

[19] Shatz, *US International Economic Strategy*, 125.

[20] Meyer and Sitaraman, "It's Economic Strategy."

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] Shatz, *US International Economic Strategy*, 130.

[25] Ibid.

[26] U.S. President, *National Cyber Strategy*, 2.

[27] Springer, "U.S. Military Professionals' Guide."

[28] TRADOC, TRADOC Pamphlet 525-3-1, xi.

[29] Ibid., 18.

[30] Ibid., 15.

GLOSSARY

Competition. The condition when two or more actors in the international system have incompatible interests but neither seeks to escalate to open conflict in pursuit of those interests. While violence is not the adversary's primary instrument in competition, challenges may include a range of violent instruments including conventional forces with uncertain attribution to the state sponsor.[1]

Crypto-asset. Digital asset implemented using cryptographic techniques.[2]

Cryptocurrency. Crypto-asset designed to work as a medium of value exchange**.** Note 1 to entry: cryptocurrency involves the use of decentralized control and strong cryptography to secure transactions, control the creation of additional assets, and verify the transfer of assets.[3]

Cryptography. Discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.[4]

Decentralized system. Distributed system wherein control is distributed among the persons or organizations participating in the operation of the system. Note 1 to entry: In a decentralized system, the distribution of control among persons or organizations participating in the system is determined by the system's design.[5]

Digital asset. Asset that exists only in digital form or which is the digital representation of another asset.[6]

Digital currency. Includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency.[7]

Distributed ledger technology oracle/DLT oracle/oracle - service that updates a (Garamone 2019) (Nakasone 2019)distributed ledger (3.22) using data from outside of a distributed ledger system (3.30). Note 1 to entry: DLT oracles are useful for smart contracts (3.72) that cannot access sources of data external to the distributed ledger system (3.30).[8]

Encryption. A technique securing data by scrambling the data . . . in a such a way that the message can be recovered by a person possessing a secret code called a key. The requirements for a good encryption scheme include protecting the classic elements of computer security : authenticity, integrity, and confidentiality. An encrypted message can be stored or transmitted to another point with a reasonable expectation of security, even if the medium used to transmit it is not secure, e.g. the Internet. Integrity can be assured through a similar technique called hashing. Hashing produces a unique signature of the original data, like a fingerprint. At the other end of the transmission, a new hash is calculated by the recipient of the data and compared to the sender's hash. If they match, the data have not been altered.

A public key/private key system allows a user to authenticate data by matching a key – the only way to decode the data – with a well-known and publicly available key . . . Using these three techniques together provides a reasonable expectation that the message is private and unaltered.[9]

---

[1] TRADOC, TRADOC Pamphlet 525-3-1, GL-2.

[2] International Organization for Standardization, "Blockchain and distributed ledger technologies – Vocabulary," https://www.iso.org/obp/ui/#iso:std:iso:22739:dis:ed-1:v1:en.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] U.S. Department of the Treasury, "Financial Sanctions: Frequently Asked Questions," https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs.

[8] Ibid.

[9] Taylor et al., *Cyber Crime and Cyber Terrorism*, 369.

BIBLIOGRAPHY

Alex077. "Russia Will Issue Its Own Cryptocurrency – the Cryptoruble." Bitnovosti.com. October 16, 2017. https://bitnovosti.com/2017/10/16/rossiya-vypustit-sobstvennuyu-kriptovalyutu-kriptorubl/.

Alizar. "Putin has Ordered a Russian Cryptocurrency be Issued: The Cryptoruble." *Geek Times*. October 15, 2017. https://geektimes.ru/post/294373.

Altcoin.info. "Cryptoruble: What Is It And What Will It Be Like?" October 16, 2017. https://altcoin.info/news/kriptoruble-chot-eto-takoe-i-kakim-on-budet-872.html.

Arbatova, Nadezhda. "Three Faces of Russia's Neo-Eurasianism." The International Institute for Strategic Studies. December 2019. https://www.iiss.org/ publications/survival/ 2019/survival-global-politics-and-strategy-december-2019january-20.

Ashmanov, Igor. "The Recipe for Digital Sovereignty." *Rossijskoe Agentstvo Novostej.* August 22, 2017. http://www.ru-an.info/.

Balakirev.ia. "The Authorities Offer A Cryptoruble." *Vedomosti.* October 18, 2017. https://www.vedomosti.ru/comments/economics/articles/2017/10/18/738302-vlasti-predloshit-kriptorubl#/.

Bank of Russia. "Bank of Russia and Market Participants Have Developed Masterchain Prototype and Successfully Made First Test Transactions," October 5, 2016, https://www.cbr.ru/eng/press/event/?id=643.

Baulin, A. "Will Blockchain Online Become The Distribution Register for a New Economic Idea?" *Forbes*. October 31, 2017. http://www.forbes.ru/tehnologii/ 351861-blokcheyn-v-efire-stanet-li-raspredelennyy-reestr-novoy-ekonomicheskoy-ideey.

Baydakova, Anna. "'Disappointed' by Central Bank Blockchain, Russia's Largest Bank Eyes Alternatives." Yahoo Finance. July 2, 2019. https://finance.yahoo.com/ news/russia-largest-bank-quitting-central-080038612.html.

Berkebile, Richard. "Thoughts on Force Protection." *Joint Forces Quarterly* 81 (2nd Quarter 2016): 145.

Besedovala, Irina. "The Yarovaya Laws Will Save Us from the CIA." *Fontanka.* October 22, 2016. http://www.fontanka.ru/2016/10/22/061/.

Bitcoin.com. "US Excludes Iran's Central Bank from the Global Financial System." November 9, 2018. https://news.bitcoin.com/us-excludes-irans-central-bank-from-the-global-financial-system/.

Blackwill, Robert D., and Jennifer M. Harris. "The Lost Art of Economic Statecraft: Restoring an American Tradition." *Foreign Affairs* (March/April 2016). https://www.foreignaffairs.com/articles/2016-02-16/lost-art-economic-statecraft?cid=nlc-fatoday-20160226.

Bobylev, Sergey. "Vladimir Putin Signs Updated National Security Strategy of the RF." *TASS.* December 31, 2015. https://tass.ru/politika/2568006.

Bond, Ian, Christian Odendahl, and Jennifer Rankin. *Frozen: The Politics and Economics of Sanctions against Russia*. Policy Brief. London, UK: Center for European Reform, March 2015.

Cau, Enrico. "The Geopolitics of the Beijing-Moscow Consensus." *The Diplomat.* January 4, 2018. https://thediplomat.com/2018/01/the-geopolitics-of-the-beijing-moscow-consensus/.

Chen Aizhu, Shu Zhang, Florence Tan, Muyu Xu, Timothy Gardner, Jeff Mason, and Parisa Hafezi. "China continued Iran oil imports in July in teeth of U.S. sanctions: analysts." *Reuters*. August 8, 2019: https://www.reuters.com/article/us-china-iran-oil/china.

Conley, Heather. "Drivers and Ramifications of US Sanctions Policy Towards Russia." SMA General Speaker Series, Center for Strategic and International Studies, October 10, 2019. https://nsiteam.com/drivers-and-ramifications-of-us-sanctions-policy.

Cryptorussia. "Putin Has Decided Russia Will Issue its Own Cryptocurrency." October 14, 2017. https://cryptorussia.ru/news/ putin-prinyal-reshenie-o-tom-chto-rossiya-vypustit-svoyu-kriptovalyutu.

Dawisha, Karen. "The Putin Principle: How It Came to Rule Russia." *World Affairs Journal* (May/June 2015): 14-22.

Dobbins, James. "Nonviolent Ways the United States Could Exploit Russian Vulnerabilities." The RAND Corporation. April 24, 2019. https://www.rand.org/news/press/2019/04/24.html.

Dobbins, James, Raphael S. Cohen, Nathan Chandler, Bryan Frederick, Edward Geist, Paul DeLuca, Forrest E. Morgan, Howard J. Shatz, and Brent William. *Overextending and Unbalancing Russia: Assessing the Impact of Cost-Imposing Options*. Santa Monica, CA: RAND Corporation, 2019.

Early, Bryan R., and Keith Preble. "'Sanctions Busting': The Risks and Rewards to those Trying to Circumvent the System." SanctionsAlert.com. June 15, 2018. https://sanctionsalert.com/sanctions-busting-the-risks-and-rewards-to-those-trying-to-circumvent-the-system/.

Elliott, Kimberly Ann. "Evidence on the Costs and Benefits of Economic Sanctions." Speech given before the Subcommittee on Trade, Committee on Ways and Means, United States House of Representatives." Peterson Institute for International Economics. Washington, DC, October 23, 1997.

Ellis, R. Evan. "Russian Activities in Latin America." In *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper,* edited by Nicole Peterson, 76-81. Washington, DC: Department of Defense, Joint Chiefs of Staff, Freedom's Fortress, May 2019.

Federal Republic of Brazil, Russian Federation, Republic of India, People's Republic of China, and Republic of South Africa. Treaty for the Establishment of a BRICS Contingent Reserve Arrangement, Fortaleza, Brazil July 15, 2017. BRICS Information Center. http://brics.itamaraty.gov.br/media2/press-release/220-treaty-for-the-establishment-of-a-brics-contingent-reserve-arrangement-fortaleza-july-15.

Financial Crimes Enforcement Network, U.S. Treasury. "Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium." New York, NY, November 15, 2019. https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-chainalysis-blockchain-symposium.

Finch, Raymond. "The Kremlin's Economic Checkmate Maneuver." *Problems of Post-Communism*, 62 (2015): 188.

Frankenfield, Jake. "CryptoRuble." Investopedia. June 25, 2019. https://www.investopedia.com/terms/c/cryptoruble.asp.

Frebowitz, Ryan L. "Cryptocurrency and State Sovereignty." Technical Report, Naval Postgraduate School, Monterey, CA, 2018.

Garamone, Jim. "European Command Exercise Program Aims to Deter Russia." U.S. Department of Defense. June 3, 2019. https://www.defense.gov/explore/story/Article/1864862/european-command-exercise-program-aims-to-deter-russia/.

Gleason, Gregory. "Currency Wars along the Silk Road. Which will emerge on top in Central Asia: The dollar, the yuan, or even Bitcoin?" *The Diplomat.* July 27, 2017. http://thediplomat.com/ 2017/07/currency-wars-along-the-silk-road/.

_____. "FSB Seeks to Forge 'Digital Sovereignty' in Russia's Financial Sector." *Eurasia Daily Monitor* 14, no. 109 (2017). https://jamestown.org/program/fsb-seeks-to-forge-digital-sovereignty-in-russias-financial-sector/.

_____. "Uzbekistan: Evaluating the Chances for a Convertible Currency." *Eurasianet.* August 4, 2017. http://www.eurasianet.org/node/84651.

Goncharov, Aleksandr. "A Cryptoruble May Be Created in Russia in 2017 – Myth or Reality? The Experts Give Their Opinions." *Gazeta-Pravo*. November 7, 2017. http://gazeta-pravo.ru/v-2017-godu-v-rossii-mozhet-byt-sozdan-kriptorubl-mif-ili-realnost-mnenie-ekspertov/.

Gordon, Gary R., Chet D. Hosmer, Christine Siedsma, and Don Rebovich. "Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime." Research Report. Document No. 198421. Study sponsored by the National Institute of Justice, February 4, 2002.

Greenwald, Michael. "Russia and China Are Hard Targets for U.S. Sanctions. That Could Be a Problem." *Barron's*. February 29, 2020. https://www.barrons.com/articles/russia-and-china-are-hard-targets-for-u-s-sanctions-that-could-be-a-problem-51582986656.

Gutterman, Ivan, Wojtek Grojec, and RFE/RL's Current Time. "A Timeline Of All Russia-Related Sanctions. A detailed look at all the sanctions levied against Russia, and its countersanctions, since 2014." *Radio Free Europe Radio Liberty.* September 19, 2018. https://www.rferl.org/a/russia-sa.

Headquarters, Department of the Army. Army Regulation 25-2, *Information Management: Army Cybersecurity*. Washington, DC: Government Publishing Office, April 4, 2019.

Helms, Kevin. "Russian Cryptocurrency Bill Is Ready – Regulators Share Details." Bitcoin.com. December 29, 2017. https://news.bitcoin.com/russian-cryptocurrency-bill-ready/.

Hendrix, Cullen S. "Freezing Iran Out of Oil Markets Won't Work." *Denver Post.* August 13, 2018. https://www.piie.com/commentary/op-eds/freezing-iran-out-oil-markets-wont-work.

Hitchens, Theresa. "US Urges 'Like-Minded' Countries To Collaborate On Cyber Deterrence." *Breaking Defense*. April 24, 2019. https://breakingdefense.com/2019/04/us-urging-likeminded-countries-to-collaborate-on-cyber-deterrence/.

Hyland-Wood, David, and Shahan Khatchadourian. "A Future History of International Blockchain Standards." *The Journal of The British Blockchain Association* 1 (June 2018). https://www.researchgate.net/publication/326081291, DOI: 10.31585/jbba-1-1-(11)2018.

International Institute for Strategic Studies. "War, power, rules." Accessed December 12, 2019. https://www.iiss.org/research/war-power-rules.

International Organization for Standardization. "Blockchain and distributed ledger technologies - Vocabulary." https://www.iso.org/obp/ui/#iso:std:iso:22739:dis:ed-1:v1:en.

Jones, Gavin. “Italy PM says is working to try to end sanctions against Russia.” *Reuters*. March 8, 2019. www.reuters.com.

Kakushadze, Zura, and Jim Kyung-Soo Liew. “CryptoRuble: From Russia with Love.” SSRN. Last updated January 26, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3059330.

Koroleva, A. “The cryptoruble will be a blow to the existing payment system.” Expert Online. October 17, 2017. http://expert.ru/2017/10/17/kriptoruble-udarit-po-platezhnyim-sistemam/.

Kosseff, Jeff. “The Contours of ‘Defend Forward’ Under International Law.” 11th International Conference on Cyber Conflict: Silent Battle. Edited by T. Minarik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, and G. Visky. Tallinn: NATO CCD COE Publications, 2019.

Kripto-Rubl. “Cryptoruble: What is it, Can I Buy it, When Are They Issuing it, and How Can I Use it to Make Money?” October 24, 2017. https://kripto-rubl.ru.

Leary, Kyree. “Vladimir Putin Just Revealed Russia’s Plans for Cryptocurrencies.” *Futurism.* October 26, 2017. https://futurism.com/vladimir-putin-just-revealed-russias-plans-for-cryptocurrencies/.

Lebedev, Dmitriy. “Digital Sovereignty à la Russe.” Open Democracy. November 3, 2017. https://www.opendemocracy.net/od-russia/dmitry-lebedev/digital-sovereignty-a-la-russe.

Lenta. “Bit-Cohen Brothers: A New Golden Bubble.” August 22, 2017. https://lenta.ru/articles/2017/08/22/bitok.

Macaulay, T. “How Governments around the World Are Using Blockchain.” Computerworld. July 23, 2018. https://www.computerworlduk.com/galleries/applications/how-governments-are-using-blockchain-3680393/.

Mahdavieh, Rose. “‘Governments’ Adoption of Native Cryptocurrency: A Case Study of Iran, Russia, and Venezuela.” Honors Undergraduate Thesis, University of Central Florida, Orlando, FL, 2019. https://stars.library.ucf.edu/honorstheses/502.

Maslov, Aleksey. “Why ‘Cold in Economics’?” *Rossijskaya*. March 31, 2016. https://www.rg.ru/2016/03/31/reg-sibfo/kitaj-investirujet-sibir.html.

Mavadiya, Madhvi. “Putin and Ethereum: A Match Made In Fintech.” *Forbes*.August 29, 2017. https://www.forbes.com/sites/madhvimavadiya/2017/08/29/putin-ethereum-fintech/#76e2a6f16b5c.

Meduza. “Bitcoin, tokens, blockchain…Everyone pretends they understand, but I don’t.” July 17, 2017. https://meduza.io/cards/bitdoin-tokeny-blokcheyn-vse-delayut-vid-chto-razbirayutsya-v-etom-a-ya-ne-ponimayu-pomogite.

Nakasone, Paul M. “A Cyber Force for Persistent Operations.” *Joint Force Quarterly*, no. 92 (1st Quarter 2019): 10-14.

Naumov, Fyodor. “Digital Sovereignty: Why The Government Needs The Cryptoruble.” *Forbes.* November 3, 2017. http://www.forbes.ru/finansy-i-investicii/352381-cifrovoy-suvernitet-zachem-pravitelstvu-ponadobitsya-kriptorubl.

Negodiay. “Can a State Cryptocurrency Compete With Bitcoin?” Tradernet. October 16, 2017. https://tradernet.com/feed/postId/1086632.

Nepop, Liubov. “Is it time for Europe to excuse Russia’s aggression?” *Euractive.* September 25, 2015. www.euractiv.com.

Newlin, Cyrus. “U.S. Sanctions against Russia: What You Need to Know.” Center for Strategic and International Studies. October 31, 2018. https://www.csis.org/analysis/us-sanctions-against-russia-what-you-need-know.

Obozrevatel.com. “Putin Has Thought Up A Clever Way to Get around Sanctions; Alarms Are Ringing In The West.” January 3, 2018. https://www.obozrevatel.com/economics/business-and-finance/putin-pridumal-hitryij-sposob-obojti-sanktsii-na-zapade-zabili-trevogu.

Office of the Director of National Intelligence. *Global Trends: Paradox of Progress*. Washington, DC: National Intelligence Council, 2017. www.dni.gov/nic/globaltrends.

_____. *National Intelligence Strategy of the United States of America.* Washington, DC: Director of National Ingelligecen, 2019.

Palmer, Daniel. “North Korea Stole $2 Billion in Crypto and Fiat to Fund Weapons Programs.” *Coindesk*. August 6, 2019. https://www.coindesk.com/north-korea-stole-2-billion-in-crypto-and-fiat-to-fund-weapons-programs.

Pan, David. “Iran President: We Need a Muslim Cryptocurrency to Fight the US Dollar.” Coindesk. December 19, 2019. https://www.coindesk.com/iran-president-we-need-a-muslim-cryptocurrency-to-fight-the-us-dollar .

Paraskova, Tsvetana. “Venezuela to Launch Oil-Backed Petro Cryptocurrency within Days.” OilPrice.com. December 29, 2017. https://oilprice.com/Energy/Crude-Oil/Venezuela-To-Launch-Oil-Backed-Petro-Cryptocurrency-Within-Days.html.

Pocheptsov, Georgiy. “How Influence Operations, Mass Culture, and Social Media Construct a New Reality.” Noravank. May 8, 2018. www.noravank.am/rus/articles/detail.php?ELEMENT_ID=16944&print=Y.

Pomerleau, Mark. “Is there such a concept as ‘cyber deterrence?’.” *FifthDomain*. April 30, 2019. https://www.fifthdomain.com/dod/2019/04/30/is-there-such-a-concept-as-cyber-deterrence/.

Popper, Nathaniel, and Matthew Rosenberg. “How Russian Spies Hid behind Bitcoin in Hacking Campaign.” *New York Times*, July 13, 2018. https://www.nytimes.com/2018/07/13/technology/bitcoin-russian-hacking.html.

Pravda. “An unusual Way of Getting around Sanctions Has Been Named.” December 12, 2017. https://www. pravda.ru/news/ economics/12-12-2017/1360371-crypto-0/.

President of Russia. “President’s Address to the Federal Assembly.” Moscow, Kremlin, December 1, 2016. http://kremlin.ru/events/president/transcripts/messages/53379.

Pynnöniemi, Katri. “Russia’s National Security Strategy: Analysis of Conceptual Evolution.” *Journal of Slavic Military Studies* 31, no. 2 (2018): 240-256. https://www.tandfonline.com/doi/full/10.1080/13518046.2018.1451091?scroll=top&needAccess=true.

Ratna, Tanvi. “Iran Has a Bitcoin Strategy to Beat Trump.” *Foreign Policy*, January 2020. https://foreignpolicy.com/2020/01/24/iran-bitcoin-strategy-cryptocurrency-blockchain-sanctions/.

Rennack, Dianne E., and Cory Welt. “U.S. Sanctions on Russia: An Overview.” *In Focus.* Congressional Research Service. January 2, 2019. www.crs.gov.

RIA Novosti. “MinComSvyazi: We Need Digital Sovereignty to Develop the Economy.” September 5, 2017. https://ria.ru/soceity/20170905/1501809181.html.

Russian RT. “FT: Russia Is Looking For A Way to “Cut Off” Cryptocurrencies.” January 2, 2018. https://russian.rt.com/inotv/2018-01-02/FT-Rossiya-ishhet-sposob-ukrotit.

RWR Advisory Group LLC. “Monthly Report on Developments in the Economic and Financial Threat Domain, EAST ASIA August 2019: Assessing the Soft Power Projection Strategies of Key Russian State-Controlled Enterprises and Other Transactional Components of the Economic and Financial Threat Domain.” Prepared for United States European Command’s Russia Strategic Initiative, September 3, 2019.

Seddon, Max. “Russian Banker Warns Against New US Sanctions.” *Financial Times.* December 24, 2017. https://www.ft.com/content/9c25c852-e400-11e7-97e2-916d4fbac0da.

Serebryaniy, Igor. “Why does Russia need the cryptoruble? Experts Are In Disbelief.” *Rambler*. October 16, 2017. https://news.rambler.ru/markets/38165540-eksperty-obyasnili-neobhodimosti-sozdaniya-kriptorublya/?updated.

Severin, Malin. “Russian Activities in Africa (Continued).” In *Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper,* edited by Nicole Peterson, 70-75. Washington, DC: Department of Defense, Joint Chiefs of Staff, Freedom’s Fortress, May 2019.

Shatz, Howard J. *US International Economic Strategy in a Turbulent World*. Santa Monica, CA: RAND Corporation, 2016.

Smart-Lab. “Cryptocurrencies Will Be Controlled By the Government.” October 11, 2017. https://smart-lab.ru/tag.

_____. “Head of MinComSvyazi RF Nikolay Nikiforov Has Found a Replacement for the Idea of a Cryptoruble,” November 8, 2017. https://smart-lab.ru/tag.

_____. “Sergey Glazyev Explains How a Cryptocurrency Will Help Russia Get around Sanctions.” December 13, 2017. https://smart-lab.ru/tag.

Smirnova, Yekaterina, and Yelena Mukhametshina. “FSB Helping Develop an International Blockchain Standard: This will allow Russian state bodies to use the new technology in the future.” *Vedomosti*. August 18, 2017. https://www.vedomosti.ru/technology/articles/2017/ 08/18/730045-fsb-blokcheina.

Sokolova, Vera. “Crypto Way around Anti-Russian Sanctions: Crimea May Become the First Official Blockchain Zone in the World.” *Svpressa* (blog). September 1, 2017. http://svpressa.ru/blogs/article/180575.

Springer, Chris. “U.S. Military Professionals’ Guide to Understanding Strategy.” U.S. Army Command and General Staff College, Fort Leavenworth, KS.

Szakonyi, David. “Governing Business: The State and Business in Russia.” Foreign Policy Research Institute. January 22, 2018. https://www.fpri.org/article/2018/01/governing-business-state-business-russia/.

TAdvisor. “Masterchain Russian national blockchain network.” http://tadviser.com/index.php/Product:Masterchain_Russian_national_blockchain_network.

TASS. “Moiseev Suggests Using the Term ‘Cyberruble’ Instead of ‘Cryptoruble’.” November 15, 2017. http://tass.ru/ekonomika/4730204.

Taylor, Megan. “Russia Picks Prime Bitcoin Mining Territory as CryptoRuble Launch Nears.” *Bitsonline*. November 18, 2017. https://bitsonline.com/russia-bitcoin-mining-cryptoruble/.

Taylor, Robert W., Eric J. Fritsch, John Liederbach, and Michael R., Tafoya, William L. Saylor. *Cyber Crime and Cyber Terrorism*. New York: Pearson, 2019.

Teknoblog. “Cryptocurrencies: The Ideal Way to Get around Sanctions.” *Teknoblog* (blog). December 18, 2017. https://teknoblog.ru/2017/12/18/85669.

Telley, Chris. “A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency.” *Small Wars Journal* (January 2018). http://smallwarsjournal.com/print/82568.

U.S. Army Training and Doctrine Command (TRADOC). TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*. Fort Eustis, VA: TRADOC, 2018.

U.S. Army Training and Doctrine Command (TRADOC) G-2. *The Operational Environment and the Changing Character of Future Warfare.* Fort Eustis, VA: TRADOC, 2017. https://community.apan.org/wg/tradoc-g2/mad-scientist/m/visualizing-multi-domain-battle-2030-2050/200203.

U.S. Army Training and Doctrine Command and U.S. Army Futures Command. “Potential Game Changers through 2050 (The Era of Contested Equality).” Broadsheet. July 25, 2019.

U.S. Congress. Senate. “Foreign Cyber Threats to the United States.” Joint Statement for the Record to the Senate Armed Services Committee by The Honorable James R. Clapper, Director of National Intelligence; The Honorable Marcel Lettre, Undersecretary of Defense for Intelligence; and Admiral Michael S. Rogers, Commander U.S. Cyber Command, Director National Intelligence Agency; January 2017.

_____. “Statement of General Paul M. Nakasone Commander U.S. Cyber Command before the Senate Committee on Armed Services.” February 14, 2019. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.

_____. “Worldwide Threat Assessment.” Statement for the Record by James R. Clapper, Director of National Intelligence. *Hearing before the Select Committee on Intelligence*. 113th Cong., 1st sess., March 12, 2013.

U.S. Department of Defense. *Summary: Department of Defense Cyber Strategy.* Washington, DC: Department of Defense, 2018.

U.S. Department of Defense, Chief Information Office. Department of Defense Instruction No. 8500.01, Incorporating Change 1. Subject: Cybersecurity. Washington, DC, October 7, 2019.

U.S. Department of the Treasury. “Economic Policy.” https://home.treasury.gov/policy-issues/economic-policy.

_____. “Financial Sanctions: Frequently Asked Questions.” https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs.

_____. “Office of Foreign Assets Control – Sanctions, Programs, and Information.” https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

U.S. Department of the Treasury. “Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela.” Press Release. March 11, 2019. https://home.treasury.gov/news/press-releases/sm622.

_____. “Treasury Targets Attempted Circumvention of Sanctions.” Press Release. August 21, 2018. https://home.treasury.gov/news/press-releases/sm462.

U.S. Department Office of Foreign Assets Control. “Ukraine/Russia-Related Sanctions Program.” Last updated June 16, 2016.

U.S. Joint Chiefs of Staff. *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*. Washington, DC: Department of Defense, July 14, 2016. http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.

U.S. President. *National Cyber Strategy of the United States of America.* Washington, DC: The White House, September 2018.

_____. *National Security Strategy of the United States of America*. Washington, DC: The White House, December 2017.

Ward, Orla, and Sabrina Rochemont. “Understanding Central Bank Digital Currencies (CBDC). An addendum to ‘A Cashless Society – Benefits, Risks, and Issues (Interim paper)’.” Institute and Faculty of Actuaries, London, UK, March 2019.

The Washington Post. “How does Iran plan to get around US sanctions? Use other currencies.” September 30, 2018.

Welt, Cory, Kristin Archick, Rebecca M. Nelson, and Dianne E. Rennack. *U.S. Sanctions on Russia*. Congressional Research Service Report for Congress, R45415. Washington, DC: Library of Congress, January 11, 2019. https://crsreports.congress.gov.

The White House. “White House National Economic Council.” https://obamawhitehouse.archives.gov/administration/eop/nec.

Williams, Brett T. “The Joint Force Commander’s Guide to Cyberspace Operations.” *Joint Force Quarterly* (2nd Quarter 2014): 12-19.

Wood, Miranda. “Russia to confiscate crypto, central bank against private digital currency.” *Ledger Insights*. November 8, 2019. https://www.ledgerinsights.com/russia-confiscate-crypto-private-digital-currency/.

Yeremina, Nataliya. “MinCom: ‘Russia is Fated to Create the Cryptoruble’.” *Gazeta.* October 18, 2017. https://www.gazeta.ru/business/2017/10/18/10948682.shtml?updated.

Zennie, Michael. “Here’s Why Russian Bombers Are in Venezuela. And Why the U.S. Is So Angry about It.” *MSN*. December 14, 2018. http://www.msn.com/en-us/news/world/heres-why-russian-bombers-are-in-venezuela-and-why-the-us-is-so-angry-about-it/ar-BBQV0FI?ocid=ientp.