REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
03-05-2018	Paper Awards Submission	Sep 17 - May 18

4. TITLE AND SUBTITLE
The New Game: Cryptocurrency Challenges US Economic Samctions

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Deane R. Konowicz, Lt Col, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

8. PERFORMING ORGANIZATION 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 **Distribution Statement A: Approved for public release**

13. SUPPLEMENTARY NOTES
B. Franklin Reinauer II Defense Economics Prize

14. ABSTRACT
The recent creation and rapid rise of cryptocurrencies like Bitcoin present a credible means for nations, corporations, and individuals to circumnavigate and undermine economic sanctions imposed by the United States. This paper outlines five cryptocurrency strategies that are enabling countries to elude US economic sanctions. In assessing these strategies, Russia, North Korea, Venezuela, Iran, and Sudan illustrate different applications of cryptocurrencies for the same intent, to avoid sanctions. The US Government must begin to systematically address this dynamic currency evolution with an aggressive counter strategy or face the reduced effectiveness of its favorite economic instrument of power.

15. SUBJECT TERMS
Cryptocurrency, Economic Sanctions, Blockchain

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**		20	**19b. TELEPHONE NUMBER** *(Include area code)*

Reset

The New Game: Cryptocurrency Challenges US Economic Sanctions

Deane R. Konowicz

A paper submitted to the Faculty of the United States Naval War College Newport, RI in partial satisfaction of the requirements of the Department of National Security Affairs.

February 8, 2018

Contents

The recent creation and rapid rise of cryptocurrencies like Bitcoin present a credible means for nations, corporations, and individuals to circumnavigate and undermine economic sanctions imposed by the United States. This paper outlines five cryptocurrency strategies that are enabling countries to elude US economic sanctions. In assessing these strategies, Russia, North Korea, Venezuela, Iran, and Sudan illustrate different applications of cryptocurrencies for the same intent, to avoid sanctions. The US Government must begin to systematically address this dynamic currency evolution with an aggressive counter strategy or face the reduced effectiveness of its favorite economic instrument of power.

BACKGROUND

The US has increasingly used economic sanctions as its primary means to achieve national security objectives. Economic sanctions stand as valued national security tools for their relatively low cost to the treasury (as compared to military force), and because of their low domestic political costs. Since the end of the Cold War, economic sanctions have varied in effectiveness. Sanctions are designed to achieve their economic intent relative to the US backed international monetary system, in which the dollar remains the global reserve currency. Cryptocurrencies create a new and unique problem for enforcing economic sanctions for three reasons. First, cryptocurrencies allow for user anonymity through highly encrypted blockchain technology. Secondly, cryptocurrencies currently lack a sovereign central authority that can be influenced, coerced, compelled, or deterred. Lastly, the US and its allies host the primary free market exchanges that allow cryptocurrencies to exist and thrive. Therefore, placing limits on, or controlling digital currency, runs counter value to liberal democracies' free market economic principles. The primary drawbacks of these currencies are the inconsistent conversion processes

to fiat currencies and significant price volatility. Regardless of these downsides, cryptocurrencies present a viable alternative to those facing US sanctions.

The United States uses its economic instrument of power to impose economic sanctions as a means to punish, because the US proved unable to deter an unfavorable action or induce a favorable action. In their recent book, *War by Other Means: Geoeconomics and Statecraft*, Robert Blackwill and Jennifer Harris contend, "the dollar's continued universality and America's central role in financial markets, the U.S. Treasury department is able to deliver a credible ultimatum to international banks."[1] Additionally, they suggest that, "each time the United States uses sanctions, Washington may be hastening other countries' search for alternatives to the dollar, which in turn would undercut the future effectiveness of sanctions."[2] A myriad cryptocurrencies emerged in the last five years and the recent spike in value introduced legitimate concerns about usage by state entities and affiliates to avoid sanctions, traditionally enforced by restricting access to the dollar.

The United States imposes economic sanctions for a host of reasons. Russia's Crimea invasion 2014, meddling in US elections, human rights violations, cybercrime, and weapons transfers to Syria, collectively led to its sanctioning in 2017. North Korea faces economic sanctions for their development of a nuclear weapons program, which violates the Nuclear Non-Proliferation Treaty and various United Nations resolutions. The US sanctioned Venezuela for its steady erosion of democratic governance, while sanctioning Iran for its ballistic missile program and state sponsorship of terrorism. Similarly, Sudan remains under US sanctions for state sponsored terrorism and human rights violations. In each of these cases, the context of the geopolitical situation largely drives the type of sanctions.

In order to understand how cryptocurrency enables cheating on sanctions by a state and its citizens, one must consider the cryptocurrency markets, national security policy decisions tied to currency use, and the dark arts of cyber hacking and money laundering. Most cryptocurrency research has focused on money laundering by criminal organizations, primarily used to maintain anonymity. However, very little research exists in understanding the use of cryptocurrencies by states for sanction avoidance. This is in part due to an exponential growth in digital currency since 2015.

Since the advent of Bitcoin in 2009, many doubted the saliency of digital currency. In 2017, the cryptocurrency market value peeked at just over $660 billion, which exceeds the market capitalization of America' largest technology companies.[3] Additionally, in excess of 100,000 global merchants now accept digital currency as payment, making financial markets take notice beyond their short-term investment value.[4] As described previously, anonymity through highly encrypted blockchain technology encompasses cryptocurrencies' main attraction. Blockchain is best defined as "a decentralized network of synchronized online registries that track the ownership and value of each token."[5] Accordingly, a digital currency's security is purely a factor of the encryption security in the underlining blockchain algorithm.[6] This encryption creates a vulnerability that may very well in time, undermine certain digital currencies and potentially create uncertainty in the entire market. To be sure, the rapid rised of cryptocurrencies has led to a greater understanding of this technology by investors and the public at large, thus increasing its acceptance. A concise distinction between cash and digital currency is as follows:

> Unlike with cash, all cryptocurrency transactions are recorded. That makes them perfectly trackable, so it's easy to monitor dealings between legitimate businesses. However, the problem is that ownership of virtual cash isn't necessarily attributable to people or businesses. And digital currency units can be anonymized by putting them through what's known as a tumbler, a service

> that changes the owner's identity by exchanging the tokens with ones belonging to other users also seeking anonymity.[7]

In addition to anonymity, cryptocurrencies pose another major challenge to the US Government in that they lack a sovereign central authority that can be acted upon.

CRYPTOCURRENCY STRATEGIES TO AVOID SANCTIONS

Russia, North Korea, Venezuela, Iran, and Sudan currently face US economic sanctions. In these countries, digital currency use has steadily increased as a means to work around those sanctions. Still one finds markedly different approaches and methods. At the nation-state level, these approaches can be refined into strategies. The following five strategies are not always used as deliberate, coherent approaches to avoiding sanctions, rather they represent buckets in which ideas, tactics, and techniques can be more easily grouped to study.

The first strategy for evading sanctions is theft of cryptocurrencies from exchanges and individuals through cyber hacking. Russia and North Korea have vast state controlled cyber capabilities. "Nobody does the dark side of the intent better than the Russians."[8] They are capable of accessing cryptocurrencies, while operating in the deepest parts of the dark web. "Consequently, it should be no surprise that cryptocurrencies, as an emerging asset class, are becoming a target of interest by a regime that operates in many ways like a criminal enterprise."[9] These state entities demonstrate the capacity to engage in elicit activities linked to crime. Given North Korea's documented participation in illicit drug production and illegal arms pedaling, researchers were not surprised to find them associated with digital currency theft.

Cryptocurrency theft generally occurs in two forms. The first technique is direct theft of currency through computer hacking. This past year South Korean cryptocurrency exchanges experienced repeat targeting campaigns by North Korean hackers. Luke McNamara, a cyber-

threat analyst notes, "If actors compromise an exchange itself (as opposed to an individual account or wallet) they potentially can move cryptocurrencies out of online wallets, swapping them for other, more anonymous cryptocurrencies or send them directly to other wallets on different exchanges to withdraw them in fiat currencies such as South Korean won, US dollars, or Chinese renminbi."[10] This has occurred with some regularity over the last year in South Korea and Japan. To that end, "a series of recent cyber attacks has netted North Korean hackers millions of dollars in virtual currencies like bitcoin, with more attacks expected as international sanctions drive the country to seek new sources of cash."[11] In addition to attacking exchanges, state sponsored hackers can use a myriad mainstream cyber tools that ultimately result in access to digital currency.

> Blockchain technologies have other criminal applications too. They're a gold mine for hackers with access to giant networks of computers known as botnets. A bot is a computer that has been infected with a type of virus known as a Trojan horse that allows the botnet's owner to remotely control the machine. Botnets can number in the hundreds of thousands of machines and are normally used to generate enormous traffic that can crash websites. Their disruptive power allows them to be weaponized to demand ransom money or wage political warfare. Back in 2007, Russian hackers showed the offensive capability of botnets for the first time when they attacked and briefly crashed much of tiny Estonia's e-infrastructure. Most recently, though, botnets have been put to a different use: stealing computer capacity to crack the codes of new bitcoins.[12]

The other illicit technique involves exploitation through hacking, then demanding cryptocurrency ransom to return the system to the status quo. The North Korean's collecting Bitcoin ransom payments from victims in the malware WannaCry attack that exploited vulnerabilities in the Windows operating system serves as a clear example of this method.[13] Thus, victims of the cyber attack accomplish the hard currency exchange to cryptocurrency for the attacker, subsequently ending the forensics trail.

The second emergent strategy involves cryptocurrency mining, which requires vast servers, large power availability, investment in technology, and well-developed computer

science talent, e.g. Russia. This pathway generates capital outside the global financial system as it relates to dollars vice a commodity, such as oil. "Russia, with its unique nexus of computer genius and money laundering expertise, looks set to become the new cryptocurrency world's Wild East."[14] Some assumed this strategy would benefit North Korea, given their inability to generate significant revenue, but they lack access to advanced hardware. Researchers are "skeptical the Hermit Kingdom is mining its own bitcoin — a process which requires a lot of sophisticated and specialized computers."[15] Russia's digital currency economy continues rapid expansion, transcending most economic sectors. "Legitimate bitcoin miners have to invest in expensive, power-hungry computer equipment and cut deals with power companies to buy their spare electricity. "Russian energy giants Gazprom and EuroSibEnergo recently announced that they were negotiating the sale of cheap megawatts to around 70 bitcoin-mining companies."[16] By wedding cryptocurrency producers with state-run energy companies, one can reasonably conclude the Kremlin's tacit consent.

A third strategy pursued by Russia and Venezuela, includes the creation of a national cryptocurrency, ostensibly more regulated by a central bank and backed by commodities such as gold and oil. Venezuela clearly lacks the cyber capability and sophistication to take advantage of the current cryptocurrency market. In 2017, Venezuela proposed a cryptocurrency backed by oil reserves as means to evade sanctions imposed by the Trump administration, which prohibit US banks from acquiring Venezuelan debt. President Maduro stated in January 2018 that "his government would issue nearly $6 billion of petros as a way to raise hard currency and to evade financial sanctions imposed by Washington."[17] Venezuaela plans to peg the petro to its oil exports (currently at $60 a barrel) to generate 100 million petros.[18] The question that remains to be answered, "Can holders of Petro or Neft-coin trust the Russian or Venezuelan governments to

provide accurate assessments of their reserves?"[19] A digital currency solely tied to petroleum appears to be nothing more than a blockchain encrypted oil futures contract.

Unlike Venezuela's plan to create an oil backed currency, Russia appears poised to make a more serious attempt to establish a sovereign digital currency intended for broader domestic and international utility. "At the St. Petersburg International Economic Forum in June, President Vladimir Putin announced that Russia was considering launching its own 'digital ruble' and praised the possibilities of virtual currencies."[20] To be sure, "the idea of undermining America's dominion as owner of the world's chief reserve currency appeals to Putin."[21] Furthermore, President Putin's advisor Sergi Glazyev stated that "cryptocurrencies may help Russian banks avoid international sanctions," and he has "advocated creating a digital ruble."[22] What remain to be seen are what benefits this strategy provides. Therein lies the potential that "getting out from underneath the petrodollar gives a country independence to begin building financial architecture that can be levered up over time to threaten the institutional control it helped create."[23] Accordingly, this idea of a digital currency backed by sovereign states leads to the next strategy.

The fourth strategy entails coupling multiple states to a common cryptocurrency. This is best illustrated by the BRICS, who have recently entertained the idea of a supranational BRICSCoin to combat the dollar that is backed by their own basket of currencies and gold.[24] Linking Russia to a common digital currency with China and India makes effective enforcement of financial sanctions infinitely more difficult for the United States. Furthermore, "This could create an effective hybrid currency that could easy trade and make exchange rates between BRICS states and their partnership more equitable."[25] Russian officials are promoting BRICSCoin under the auspices of trade versus sanctions evasion. "The Head of the Russian Direct Investment Fund **(**RDIF) Kirill Dmitriev has stated that the BRICS may opt to create their

own cryptocurrency for the purposes of global commerce."[26] Ultimately, the BRICS are seeking ways to undermine the dollar as "the most popular global trading and reserve currency."[27] This outcome clearly appeals to a rising China, but they may not be keen on sacrificing their sovereignty given their efforts to elevate the Yuan's global status.

A fifth strategy encourages a sanctioned state's population and business community to utilize all digital currencies freely. This hands off approach by a state risks undermining its fiat currency. The greater the impact of the sanctions on the fiat currency, the greater the risk a government may be willing to take in cryptocurrency experimentation, especially if it translates to domestic economic stability. As populations in authoritarian states seek out market regulated cryptocurrencies and accept these new domestic economies, an unintended consequence emerges in that the underlying legal structures to support this system may give companies both certainty and predictability in government institutions that did not previously exist.[28] Currency experts claim that the disadvantage of cryptocurrencies is the lack of central bank underwriting. This holds particularly true in terms of stable exchange rates, which rely heavily on central banks. However, in terms avoiding dollar-based sanctions, this may be seen by a sovereign state as a net advantage.[29] Additionally, autocratic regimes who possess highly developed cryptographic forensic capabilities see the potential in blockchain technology. It stands as a tempting means to monitor their population by linking currency directly to individuals and business enterprise. This tact increases government control and political leverage, unlike most central banks, which are limited to traditional monetary policy.

While less integrated into the global economy than Russia, Iran shows evidence of increased digital currency use by its population. Hadi Nemati, an Iranian cryptocurrency researcher stated, "In most of the world, bitcoin is more of a store of value, but in Iran it's a

utility because it gives us access to the world economy. Iranians buy bitcoin because they don't have access to international fiat currencies."[30] The Sudanese situation has perhaps the most in common with Russia, in that individuals find themselves constrained in international business transactions because of longstanding US financial sanctions. As businesses struggle to operate with limited capital flows, individuals have migrated to cryptocurrency to circumvent the state's financial structure. What Sudan, Iran and Russia share amongst the many countries highlighted by this research is that average citizens have turned to Bitcoin. In Sudan specifically, this ranges from bridal gifts and dowries to remittances from relatives given the nation's three-decade isolation from the western banking system, coupled with a weak local currency.[31] Countries like Sudan present a challenge to US authorities because the population sought out cryptocurrency to skirt sanctions, while the central government merely turns a blind eye.

The fundamental challenge for each of these cryptocurrency strategies used to avoid sanctions remains the conversion mechanism to fiat currencies. Major energy, commodity, and arms sales by sovereign states have yet to occur using only cryptocurrency. As blockchain proliferates in the global financial system, the likelihood of this first major transaction will increase. To be sure, financial institutions and governments the world over will take notice, but will they be ready to respond or will they be forced to react?

A US GOVERNMENT COUNTER STRATEGY

The US response to this rapidly developing challenge appears slow and cautious. The question stands: will the US Government create responsive and effective capabilities to combat these adversarial strategies? "So long as the United States seems reliant on financial sanctions, protecting the dollar's global role becomes all the more important."[32] A multi-lateral approach should be foundational to a US counter-strategy. International partners, to include the EU, Great

Britain, Canada, Australia, South Korea, Japan, and China must work towards common solutions for future economic sanctions to remain effective. The US should focus its international approach on partnerships with the G7 and G20, rather than the more contentious United Nations. These multilateral organizations not only focus on economic issues, they represent more closely aligned financial interests. "France's finance minister said his country would propose that the G20 group of major economies discuss regulation of bitcoin next year."[33] Given the scope and nature of this problem, "there is renewed interest from regulators in Singapore, the United States, Japan and China to have oversight in the cryptocurrency space and curb the potential of widespread money laundering and fraud."[34] Geo-economic experts contend, "the United States no longer enjoys a monopoly on where capital originates, how it is intermediated, and where it ends."[35] Cryptocurrencies represent a dynamic shift in how capital intermediates. "This fact makes U.S financial sanctions more difficult – and more reliant on multilateral diplomacy."[36] Consequently, Congress weighed in for the first time in the 2017 Russia Sanctions legislation.

> **SEC. 262. CONTENTS OF NATIONAL STRATEGY.**
> The strategy described in section 261 shall contain the following:
>
> (8) TREND ANALYSIS OF EMERGING ILLICIT FINANCE THREATS.—A discussion of and data regarding trends in illicit finance, including evolving forms of value transfer such as so-called cryptocurrencies, other methods that are computer, telecommunications, or Internet-based, cyber crime, or any other threats that the Secretary may choose to identify.[37]

Congress' direction to the Treasury for study and data gathering may represent little more than acknowledgement of the digital currency trend. The executive branch departments must lead this counter-strategy rather than merely studying the problem at congress' request.

Both the Department of the Treasury and the Federal Reserve play immensely in solving the emerging cryptocurrency problem as it relates to financial sanctions, but they cannot act alone. Some argue that new tools are not needed immediately as "Anti-money laundering laws

and the Bank Secrecy Act apply to digital currency exchanges and banks [that] handle digital currency transaction."[38] Regardless, the US should establish a cryptocurrency task force across relevant government departments and agencies to identify solutions and counter these five major strategies as they pertain to illicit state, corporate, and criminal transactions. This task force should include the Departments of the Treasury, State, Justice, and Defense since agencies varying from the IRS and NSA to the FBI and SEC have the combined talent and resources to tackle this rapidly evolving challenge. Additionally, government must partner with and leverage universities, banks, cyber security firms, and technology companies given their vast talent pool and ability rapidly adjudicate a changing market. As such, a tenant of the US strategy should be speed. Agencies should be given broad authority to respond and react as quickly as possible to threats and trends. A narrow window of opportunity exists for action while digital currency capitalization remains relatively small and disruptions to the market are likely isolated. This maneuver space could quickly generate regulatory and policy lessons learned, ultimately leading to a less reactionary approach.

The US task force should develop a comprehensive cryptocurrency counter strategy with an objective that ensures the US maintains an effective financial sanctions capability. This task force should begin by setting out a series of intermediate objectives that provide offensive and defensive measures to address each of the five strategies summarized earlier. As capabilities emerge, the US must carefully consider the second and third order effects as they relate to the US economy. At the most basic level, the US strategy for combatting cryptocurrency use in sanctions avoidance should focus its efforts on the underlying blockchain technology. This includes heavily investing in the cracking of blockchain cryptography in order to trace transactions.

> Payments on bitcoin and other currencies are attached with a traceable, cryptographic ID. Anyone can look up such an ID and see its entire history of transactions. Though the identities of users tied to IDs aren't generally known, experts with enough time and resources can, in some cases, trace them back to individuals in the real world.[39]

Another plausible counter-tactic proposes monitoring where the transactions exist to reconvert the currency, but this creates a complex web to follow, given both the volume and frequency of cryptocurrency transactions. The IRS has already engage exchanges such as Coinbase to share its customer data, demanding tax law compliance.[40] This approach opens the question as to whether the US and China share a mutual interest in limiting digital currencies to protect their fiat currencies and geo-economic power relative to illicit actions by individuals, organizations, and states. Cryptocurrencies may be perceived as a threat to both the dollar and the renminbi in the long run. Regardless, US policy makers require a robust range of capabilities and options that vary from deliberately inducing cryptocurrency market volatility to blockchain decryption.

Finally, more political pressure may push sovereign countries to regulate cryptocurrencies if fiat currencies appear threatened. An offensive part of US strategy should include developing its own cryptocurrency, backed by the dollar. This maneuver could quickly absorb significant market share, thereby forcing capital flows away from more volatile cryptocurrencies. Additionally, the US could control the blockchain encryption for a digital dollar in order to trace its use, unlike current $100 bills. As recently as November 2017, "William Dudley, president and CEO of the Federal Reserve Bank of New York, said the Fed is exploring the idea of offering its own digital currency."[41] In addition to the US, there are at least a dozen other countries reportedly considering the same. While cryptocurrencies are becoming ubiquitous across the global economy, companies in non-sanctioned countries whose business relies on customers in sanctioned countries are adapting. For example, "Ukrainian shipping company Varamar Ltd…is using Bitcoin as a way of avoiding sanctions."[42] Cross boarder trade

and commerce pose yet more questions for regulation. The inevitable patchwork of regulation by individual governments, to include the US, will ostensibly lead to further cryptocurrency volatility, perpetuating its fringe status in the short run, but not indefinitely.

CONCLUSION

The explosive emergence of cryptocurrencies clearly demonstrates a credible means for nations, corporations, and individuals to circumnavigate and undermine US imposed economic sanctions. "With tightening sanctions and usage of cryptocurrencies broadening, security experts say North Korea's embrace of digital cash will only increase."[43] Unlike North Korea, Venezuela, Iran, and Sudan, the Russians have chosen to engage in all five strategies; essentially betting on all the horses in the race, knowing that one will likely win. The US possesses the ways and means to combat these emerging strategies, but a lack of urgency and strategy will continue to embolden sanctioned states to find alternatives. Economic sanctions will only remain a highly desired and valuable national security tool if the US Government aggressively confronts the digital currency reality with a comprehensive strategy.

NOTES

[1] Robert D. Blackwill and Jennifer M. Harris. *War by Other Means*. The Belknap Press of Harvard University, Cambridge, MA, 2016: p. 58-59.
[2] Ibid, p. 59.
[3] Gertrude Chavez-Dreyfuss, Jemima Kelly, and Swati Pandey, "Exchange giant CME's bitcoin futures get tepid take-up in debut," *Reuters* (December 17, 2017).
[4] Owen Matthews, "Bitcoin and Blockchain: A Russian Money Laundering Bonanza?" *Newsweek* (September 18, 2017).
[5] Ibid.
[6] Tom Luongo, "Oil Producers Turning to Crypto to Solve Sanctions Problems." (Decemeber 11, 2017).
[7] Matthews, "Bitcoin and Blockchain: A Russian Money Laundering Bonanza?"
[8] Ibid.
[9] Luke McNamara, "Why is North Korea so interested in Bitcoin?" *FireEye.com* (September 11, 2017).
[10] Ibid.
[11] Jeremy Wagstaff, and Josh Smith. "Multi-stage cyber attacks net North Korea millions in virtual currencies: researchers." *Reuters* (December 19, 2017).
[12] Matthews, "Bitcoin and Blockchain: A Russian Money Laundering Bonanza?"
[13] Yuji Nakamura, and Sam Kim, "North Korea Is Dodging Sanctions With a Secret Bitcoin Stash." *Bloomberg Businessweek* (September 11, 2017).
[14] Matthews, "Bitcoin and Blockchain: A Russian Money Laundering Bonanza?"
[15] David Gilbert, "Bitcoin and other cryptocurrencies could help North Korea avoid the impact of international sanctions." *CuencaHighLife* (November 26, 2017).
[16] Matthews, "Bitcoin and Blockchain: A Russian Money Laundering Bonanza?"
[17] Reuters Staff, "Venezuela's Congress declares 'petro' cryptocurrency illegal," *Reuters* (January 9, 2017).
[18] Ibid.
[19] Luongo, "Oil Producers Turning to Crypto to Solve Sanctions Problems."
[20] Matthews, "Bitcoin and Blockchain: A Russian Money Laundering Bonanza?"
[21] Ibid.
[22] Jake Rudnitsky, "Vladimir Putin aide eyes cryptocurrencies to beat sanctions, Russia newswire says," *The Sydney Morning Herald* (December 13, 2017).
[23] Luongo, "Oil Producers Turning to Crypto to Solve Sanctions Problems."
[24] Adam Garrie, "In Blow to US Dollar, BRICS Consider 'Sanctions-Proof' Cryptocurrency," *Mint Press News* (September 5, 2017).

[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Luongo, "Oil Producers Turning to Crypto to Solve Sanctions Problems."
[29] Garrie, "In Blow to US Dollar, BRICS Consider 'Sanctions-Proof' Cryptocurrency."
[30] Ali Breland, "Cryptocurrencies on the rise in Iran," *The Hill* (January 10, 2018).
[31] Matina Stevis-Gridneff and Georgi Kantchev, "Bitcoin Is a Hit in Countries Where Locals Face Currency Troubles," *The Wall Street Journal* (Jan 4, 2018).
[32] Blackwill and Harris. *War by Other Means*. p. 193.
[33] Chavez-Dreyfuss, "Exchange giant CME's bitcoin futures get tepid take-up in debut."
[34] Saheli Roy Choudhury, "Governments want to control cryptocurrencies – but there's a danger to too many rules," *CNBC* (September 12, 2017).
[35] Blackwill, *War by Other Means*, p. 192.
[36] Ibid, p.192.
[37] Congress "Countering America's Adversaries Through Sanctions Act" H.R. 3364-70 (July 2017)
[38] IP Greg, "Bitcoin: Electrify Investment, Lousy Currency," *The Wall Street Journal* (December 13, 2017).
[39] Breland, "Cryptocurrencies on the rise in Iran."
[40] Taylor Hatmaker, "Coinbase ordered to give the IRS data on users trading more than $20,000," *TechCrunch.com* (November 29, 2017).
[41] Qin Chen, "Next stop in the crypto currency craze: A government-backed coin," *CNBC* (November 30, 2017)
[42] JP Buntinx, "Ukrainian Firm Looks at Bitcoin to Bypass Sanctions," *The Merkle* (December 4, 2017).
[43] Nakamura, "North Korea Is Dodging Sanctions With a Secret Bitcoin Stash."

BIBLIOGRAPHY

Blackwill, Robert D., Jennifer M. Harris. *War by Other Means*. The Belknap Press of Harvard University, Cambridge, MA, 2016.

Breland, Ali. "Cryptocurrencies on the rise in Iran." *The Hill* (January 10, 2018). http://thehill.com/policy/technology/368417-cryptocurrency-sees-popularity-rise-in-iran

Buntinx, JP. "Ukrainian Firm Looks at Bitcoin to Bypass Sanctions." *The Merkle* (December 4, 2017). https://themerkle.com/ukrainian-firm-looks-at-bitcoin-to-bypass-sanctions/

Congress "Countering America's Adversaries Through Sanctions Act" H.R. 3364-70 (July 2017)

Chavez-Dreyfuss, Gertrude., Jemima Kelly, Swati Pandey. "Exchange giant CME's bitcoin futures get tepid take-up in debut." *Reuters* (December 17, 2017). https://www.reuters.com/article/us-bitcoin-futures/exchange-giant-cmes-bitcoin-futures-get-tepid-take-up-in-debut-idUSKBN1EB04N

Chen, Qin. "Next stop in the crypto currency craze: A government-backed coin." *CNBC* (November 30, 2017). https://www.cnbc.com/2017/11/30/cryptocurrency-craze-springboards-government-backed-coin.html

Choudhury, Saheli Roy. "Governments want to control cryptocurrencies – but there's a danger to too many rules." *CNBC* (September 12, 2017). https://www.cnbc.com/2017/09/12/regulators-are-turning-their-attention-to-cryptocurrencies.html

Garrie, Adam. "In Blow to US Dollar, BRICS Consider 'Sanctions-Proof' Cryptocurrency." *Mint Press News* (September 5, 2017). http://www.mintpressnews.com/blow-us-dollar-brics-considers-cryptocurrency/231571/

Gilbert, David. "Bitcoin and other cryptocurrencies could help North Korea avoid the impact of international sanctions." *CuencaHighLife* (November 26, 2017). https://cuencahighlife.com/bitcoin-and-other-cryptocurrencies-could-help-north-korea-avoid-sting-of-international-sanctions/

Greg, IP. "Bitcoin: Electrify Investment, Lousy Currency." *The Wall Street Journal* (December 13, 2017).

Hatmaker, Taylor. "Coinbase ordered to give the IRS data on users trading more than $20,000." *TechCrunch.com* (November 29, 2017). https://techcrunch.com/2017/11/29/coinbase-internal-revenue-service-taxation/

Higgins, Stan. "Controversial US Sanctions Bill Calls for Cryptocurrency Research." *Coindesk*, (August 7, 2017). https://www.coindesk.com/controversial-us-sanctions-bill-calls-cryptocurrency-research/

Luongo, Tom. "Oil Producers Turning to Crypto to Solve Sanctions Problems." (Decemeber 11, 2017). https://tomluongo.me/2017/12/11/oil-producers-turning-to-crypto-to-solve-sanctions-problems/

Matthews, Owen. "Bitcoin and Blockchain: A Russian Money Laundering Bonanza?" *Newsweek* (September 18, 2017). http://www.newsweek.com/russia-finally-embracing-virtual-currencies-666794

McNamara, Luke. "Why is North Korea so interested in Bitcoin?" *FireEye.com* (September 11, 2017). https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html

Monterio, Brad J. "Blockchain Is the New Black No, Really." *California CP*; Redwood City Vol.85, Iss. 4, (Oct 2016): 16-18.

Nakamura, Yuji., Sam Kim. "North Korea Is Dodging Sanctions With a Secret Bitcoin Stash." *Bloomberg Businessweek* (September 11, 2017).

https://www.bloomberg.com/news/articles/2017-09-11/north-korea-hackers-step-up-bitcoin-attacks-amid-rising-tensions

Pamplin, Berkley A. "Virtual Currencies and the Implications for U.S. Anti-Money Laundering Regulations." *Utica College* (August 2014).

Reuters Staff. "Venezuela's Congress declares 'petro' cryptocurrency illegal." *Reuters* (January 9, 2017). https://www.reuters.com/article/us-venezuela-economy/venezuelas-congress-declares-petro-cryptocurrency-illegal-idUSKBN1EY2H2

Rudnitsky, Jake. "Vladimir Putin aide eyes cryptocurrencies to beat sanctions, Russia newswire says." *The Sydney Morning Herald* (December 13, 2017). http://www.smh.com.au/world/vladimir-putin-aide-eyes-cryptocurrencies-to-beat-sanctions-russian-newswire-says-20171212-h03jju.html

Sharkov, Damien. "Bitcoin Technology Can Help Russia Dodge Sanctions: MP." *Newsweek* (June 2, 2016). http://www.newsweek.com/bitcoin-technology-can-help-russia-dodge-sanctions-mp-465901

Sauer, Beate. "Virtual Currencies, the Money Market, and Monetary Policy." *International Advances in Economics Research*; Edwardsville Vol. 22 Iss. 2, (May 2016): 117-130.

Stevis-Gridneff, Matina and Georgi Kantchev. "Bitcoin Is a Hit in Countries Where Locals Face Currency Troubles." *The Wall Street Journal* (Jan 4, 2018). https://www.wsj.com/article_email/bitcoin-is-a-hit-in-countries-where-locals-face-currency-troubles-1515067201-lMyQjAxMTI4NTA1NTAwMzUyWj/

Ulmer, Alexandra., Deisy Buitrago. "Enter the 'petro': Venezuela to launch oil-backed cryptocurrency." *Reuters* (December 3, 2017). https://www.reuters.com/article/us-venezuela-economy/enter-the-petro-venezuela-to-launch-oil-backed-cryptocurrency-idUSKBN1DX0SQ

Wagstaff, Jeremy, Josh Smith. "Multi-stage cyber attacks net North Korea millions in virtual currencies: researchers." *Reuters* (December 19, 2017). https://www.reuters.com/article/us-southkorea-cyber-hackers/multi-stage-cyber-attacks-net-north-korea-millions-in-virtual-currencies-researchers-idUSKBN1ED0ZC

Webblog post. "ValueWalk: Ruskies, Sanctions, And Bitcoin – Coincidence?" *Newstex Global Business Blogs, Chatham: Newstex* (August 16, 2017).