International Journal of Humanities and Social Science Research
www.socialsciencejournal.in
ISSN: 2455-2070
Received: 17-05-2024, Accepted: 05-06-2024, Published: 27-06-2024
Volume 10, Issue 3, 2024, Page No. 30-37

Analysis of the impact of US cyber-sanctions

Vikas Bhardwaj
Department of International Studies, Jawaharlal Nehru University, New Delhi, India

Abstract
Malicious cyber activity is a major threat to America's national, economic, and personal security, with cybercriminals causing estimated losses of $57 billion to $109 billion in 2016. Since 2015, the U.S. has imposed targeted sanctions on over 300 individuals and entities involved in cyber activities, primarily those linked to Iran, Russia, and North Korea. These sanctions, established by executive orders and congressional bills, initially targeted individuals with government ties but have recently expanded to include cybercriminals. Despite their increasing use, the effectiveness of these sanctions in changing behavior is unclear. Research indicates that sanctions can be effective when applied multilaterally and strategically, but without ongoing reassessment, they risk negative outcomes. The 116th Congress proposed legislation to formalize these sanctions but has not adequately overseen their implementation or effectiveness. As other countries adopt similar measures, it is crucial for Congress to push for a comprehensive evaluation of U.S. cyber sanctions. This paper provides an analysis of cyber activities against the U.S., a history of U.S. cyber sanctions, an assessment of sanction effectiveness in foreign policy, and recommendations for Congress to improve oversight and evaluate the impact of cyber-related sanctions.

Keywords: Cyber-sanctions, Russian economy, U.S. sanctions, CSIS, cyber-crime, embargo, cryptocurrency, cyber threat

Introduction

Malicious cyber activity poses one of the greatest threats to America's national, economic, and personal security. Yet, the perpetrators of these crimes largely operate with pure impunity and face little consequences for their actions. This is particularly the case for cybercriminals who cost the US economy anywhere from $57 billion to $109 billion in 2016 alone (US White House, 2020).

Since 2015, the United States has imposed targeted sanctions (e.g., asset freezes, travel bans) on over 300 individuals and entities in response to malicious cyber activity (Thompson, 2021). Many of these sanctions were issued under the cyber-related sanctions program administered by the Department of Treasury and established by a series of Executive Orders under Presidents Obama and Trump and bills passed by Congress (US Department of State, 2020). Sanctions have largely been imposed on individuals with ties to Iran, Russia, and North Korea, and, in about half of these cases, sanctions have followed indictments. An overwhelming majority of these sanctions have targeted individuals with suspected links to government entities and, only recently, have cyber sanctions targeted cybercriminals (Thompson, 2021).

As targeted sanctions increasingly become a tool deployed by the US government to punish malicious cyber actors, it remains unclear whether they are having an impact in changing behaviour. Research on the impact of sanctions more broadly indicates that sanctions can be an effective tool to impose consequences on bad actors and change their actions when employed multilaterally, as part of a coherent strategy, and effectively messaged (David & O'Toole, 2020). However, imposing sanctions on malicious cyber actors without continuously reassessing their impact and the expected reciprocal actions by the target(s), risks a number of potentially negative outcomes.

While Congress introduced legislation in the116th Congress to impose new or codify existing cyber-related sanctions into law (US 116th Congress, 2020), it has not exercised the necessary oversight over the Executive Branch's strategy in issuing cyber-related sanctions and determining their efficacy.

With other countries now following America's lead in issuing these sanctions, the time is ripe for the new Congress to push for an inter-agency, holistic assessment of the impact of US cyber-related sanctions (Botek, 2020). And with cyber-crime increasingly threatening all sectors of the US economy, Congress must call for an evaluation as to whether sanctions on non-state cybercriminals should increasingly be used.

Analysis of the nature of cyber activity committed against the United States:

Malicious cyber activity is surging in the United States, targeting its people, undermining its national security, and affecting nearly every sector of its economy. Nearly one in four American households have fallen victim to a cybercrime (Reinhart, 2020). Entire state and local governments have been held hostage by ransomware (a form of cybercrime), resulting in millions of dollars lost in recovery costs (Newman, 2020). And now, America's hospitals and schools are being targeted in the midst of the COVID-19 pandemic (Bergal, 2020) [3]. Foreign adversaries have also leveraged cybercrime tools and employed cybercriminals to steal America's national security secrets and intellectual property (US Department of Homeland Security, 2019).

The economic losses resulting from cybercrime in the United States and globally are staggering. In 2016 alone, cybercriminals cost the US economy anywhere from $57 billion to $109 billion, according to the last White House Council on Economic Advisors assessment (US White House, The Council of Economic Advisers, 2018). Each year, the global impact also grows. In December 2020, the Center for Strategic and International Studies (CSIS) reported the cost of cybercrime reached over $1 trillion globally, which was a 50% increase from their 2018

assessment (Lewis & Zhanna, 2020). In particular, the economic losses from ransomware have continued to surge during the COVID-19 pandemic. One recent report found a 311% increase in 2020 from 2019 in cryptocurrency received by criminal addresses from ransomware for a total of just under $350 million (Chain Analysis, 2021) [5].

The perpetrators of malicious cyber activity range from state-sponsored or -enabled actors, organized criminal groups, and lone actors. One study found non-state cybercriminals conducted 57% of the largest cyber loss events in the world between 2015 and 2019. The other 43% of these attacks were perpetrated by state-sponsored or -enabled actors (Cyentia Institute, 2020). Some US assessments indicate cybercriminals are generally more motivated by financial reasons, while nation-state actors tend to be more focused on stealing, destroying, or compromising victim data (Ablon, 2018). The line between nation-state actors and non-state cybercriminals, however, has blurred as states abet and directly employ non-state cybercriminals and/or their tools (US Department of Homeland Security, 2019).

Despite the proliferation of a wide spectrum of cyber activity against the United States, the state and non-state actors committing it rarely face consequences. But sanctions have emerged as a tool increasingly used to deter and/or compel a change in their behavior. Yet compared to the number of incidents, few actors who engage in malicious cyber activity are sanctioned. Of those that are, they are largely nation-state-connected actors residing in countries that are particularly difficult for US authorities to reach.

Overview of the history of US cyber sanctions

As the number of malicious cyber incidents in the United States has grown, so too has the number of cyber sanctions (Dunn, 2020) [14]. US policymakers have used economic pressure to advance foreign policy goals and respond to threats against the nation since the dawn of the Republic, and sanctions have now increasingly, albeit sparingly, become a tool of response to malicious cyber activity. In 2015, then-President Barack Obama issued the first executive order (EO) to institute a sanctions regime targeting the individuals and entities behind "significant cyber- enabled activities" (White House, 2015). These cyber sanctions along with sanctions programs established to deal with particular countries and security threats of concern, including terrorism, have been used to target the individuals and entities behind cyberattacks and other cyber activity against the United States.

The US government imposes sanctions broadly to alter the strategic decisions of state and non-state actors that threaten US interests or in response to particularly egregious behavior. A form of sanctions was first established in 1807 when Congress passed the "Embargo Act" (Frankel, 1982). Over two centuries later, the globalization of economic markets and the desire for new tools to combat threats to national and global security has contributed to substantial innovation in the use of coercive economic measures such as sanctions. Sanctions programs have continued to grow in size and scope. They can either be comprehensive (i.e., restrictions on trade and commercial activity with an entire country) or targeted (i.e., restrictions on the activity of specific individuals and/or entities). Many federal government entities play a role in administering sanctions and tracking their implementation, including the Departments of Treasury (namely through its Office of Foreign Assets Control or OFAC), State, and Commerce (US Government Accountability Office, 2019). The Government Accountability Office (GAO) highlights that:

"Sanctions may place restrictions on a country's entire economy, targeted sectors of the economy, or individuals or corporate entities. Reasons for sanctions range widely, including support for terrorism, narcotics trafficking, weapons proliferation, and human rights abuses. Economic restrictions can include, for example, denying a designated entity access to the U.S. financial system, freezing an entity's assets under U.S. jurisdiction, or prohibiting the export of restricted items" (US Government Accountability Office, 2019).

As of December 2020, the United States has nearly 8,000 sanctions in place on individuals, companies, or entire countries (Gilsan, 2019) [15]. Of those 8,000, a little more than 300 are for malicious cyber activity (Thompson, 2020) [40].

Debate continues as to the effectiveness of sanctions overall and their impact. Critics argue that sanctions are poorly designed and rarely successful in changing a target's conduct (Fishman, 2020) [13]. And there is growing recognition that comprehensive sanctions on entire countries have contributed to a number of humanitarian crises and corruption (Omar, 2019) [32]. However, others have argued that sanctions have become more effective in recent years as they have become more targeted in nature (Hufbauer, 2014) [19]. And some research has given sanctions credit, at least in part, for changing the behavior of governments in Libya and South Africa in the past (Nephew, 2018) [30].

Broadly, the authorities for US sanctions programs may originate through executive or legislative action. Pursuant to the "International Emergency Economic Powers Act" (IEEPA, P.L. 95-223), the President, upon declaring a state of emergency, can institute sanctions by EO against countries or individuals in response to an "unusual and extraordinary" threat (US Congress. International Emergency Economic Powers Act, 1977). Congress, for its part, may also pass legislation imposing new sanctions or modifying existing ones.

Against this backdrop, the US government first started sanctioning actors accused of committing malicious cyber-enabled activity in 2012 under a number of different authorities (Thompson, 2020) [40]. Subsequently, in 2015, then-President Obama issued EO13694 (White House, 2015), later amended in 2016 to include election interference in EO13757 (US Department of Treasury, 2016), establishing a dedicated sanctions program to respond to significant malicious cyber-enabled activities with asset freezes, travel restrictions, and property and interest blocks. Lawmakers codified portions of these EOs in 2017 with the passage of the "Countering America's Adversaries Through Sanctions Act" (CAATSA, P.L. 115-44), which provides for sanctions against individuals or entities that engage in "significant activities undermining cybersecurity" on behalf of Russia (US Department of Treasury, 2017). Further, in2018,then President Trump also issued EO13848, imposing sanctions for election interference (US GPO EO 13848, 2018). These EOs and CAATSA covered several categories of activity, including foreign election interference, infiltration and/or disruption of computer networks, and misappropriation of trade secrets

stolen via cyber-enabled means (US Department of Treasury EO 13757, 2016).

Analysis of the actors US cyber sanctions have targeted

Using these and other authorities, the US government has instituted targeted sanctions on a number of individuals and entities for their malicious cyber activity. According to research by the Carnegie Endowment for International Peace and with more recent additions added since that research was finalized, the United States had imposed sanctions 35 times, targeting over 300 people and entities, in response to malicious cyber activity under several different authorities, including the cyber-related sanctions program (Thompson, 2020) [40]. (SeeAppendix1) The sanctioned activity has ranged from cyber-enabled espionage, election interference, design and distribution of destructive malware, exchanging currency gained from ransomware attacks, business email compromise, and other cyberactivity (Thompson, 2020) [40]. Preceding or simultaneous to the issuance of these sanctions, the Department of Justice has also indicted about half of these same individuals and entities, indicating that indictments can serve as an important tool allowing the US federal government to lay out the case against these actors for follow-up action such as sanctions.

The US government has predominantly deployed cyber sanctions against nation-state- connected individuals or entities in three countries: Iran, North Korea, and Russia (Thompson, 2020) [40]. Cyber sanctions have also been issued against individuals in other countries in a few select cases (US Department of Treasury, 2020). Some organizations have criticized the United States for failing to sanction Chinese cyber actors despite the tremendous amount of malicious cyber activity emanating from China (Logan, 2020) [25]. As of December 2020, some entities with business in China have been sanctioned but for facilitating individuals' evasion of US cyber sanctions (US Department of Treasury, 2020). Additionally, while the Department of Justice has indicted several Chinese citizens for malicious cyberactivity ((US Department of Justice, 2020)), only two with no suspected ties to the Chinese government have been the target of sanctions for conducting malicious cyberactivity (US Department of Treasury, 2020). In response to malicious cyberactivity emanating from China, the US government has largely pursued other actions, including diplomatic negotiations (Williams, 2018) [17].

Despite some estimates indicating non-state actors, mainly cybercriminals, accounted for over 50% of the largest cyber loss events in the world between 2015 and 2019 (Cyentia Institute, 2020), only 26 suspected non-state individuals or entities were sanctioned for cyber activity as of December 2020. (Though the increased blurring of the boundary between state and non-state actors, as states abetted and in some instances directly employed non-state cybercriminals and/or their tools to advance their objectives, makes such clear delineation difficult and should be kept in mind) (Healey, 2012) [18]. Research has shown that while sanctions on non-state actors may not change their calculus, they can have an impact on freezing these illicit actors out of legitimate financial systems in order to deny them resources (Rosenberg et. al, 2016) [37]. Sanctions can make it "costlier, riskier, [and] less efficient" for non-state actors to use and move funds (Daniel, 2011) [16]. And they may also protect the integrity of the financial system (Financial Action Task Force, 2012)

Overall, there is little to no publicly available information to indicate whether these cyber sanctions are or are not having an impact in achieving their goals. The objectives of sanctions go beyond just punishing a malicious actor and include disrupting the financing and recruiting efforts of would-be hackers and changing the long-term behavior of actors in cyberspace (Thompson, 2020) [40]. There are no publicly available assessments to indicate whether these sanctions are meeting these objectives. Further, the 2018 National Cyber Strategy makes little mention of how economic sanctions t into the US government's broader strategic approach to dealing with malicious cyber actors (US Department of Defence, 2018). This Strategy also did not establish a framework as to how decisions are being made and which actors US cyber sanctions will target, leading to concerns over inconsistent applications (Logan, 2020) [25]. In a March 2020 hearing before a House Appropriations subcommittee, then-Treasury Secretary Steven Mnuchin did not directly answer a question as to whether cyber sanctions have been effective. Mnuchin responded, "I do think our sanctions programs work, and I do think we're sanctioning the right people, and I do believe we have proper resources" (House Appropriations Subcommittee Hearing with Treasury Secretary Steven Mnuchin, 2021).

Five years after President Obama issued his first EO to establish an American cyber-related sanctions program, other countries are now following suit. Both the European Union (EU) and the United Kingdom (UK) have adopted cyber sanctions regimes closely mirroring that of the United States, though there are some noted differences (Thompson, 2020) [40]. In July 2020, the EU imposed cyber sanctions for the first time on six individuals and three entities from North Korea, Russia, and China, who are suspected to be responsible for a number of different cyberattacks and cyber espionage (Council Implementing Regulation (EU) 2020). In October 2020, the Group of Seven (G7), a forum of the world's seven leading industrial nations, stated it would explore opportunities to impose more coordinated, targeted financial sanctions in response to malicious cyber activity (Ransomware Annex to G7 Statement, 2020)

As the US government works to advocate for other countries to establish cyber sanctions regimes and coordinates multilaterally to impose sanctions, it is critical that it can demonstrate the impact of these efforts. Research on sanctions broadly can offer some important insights.

Assessment of existing research on sanctions as a tool of US foreign policy

Research on sanctions broadly as a US foreign policy tool indicates that these measures can have an impact when certain conditions are met. As the relevant federal entities work to determine whether sanctions should increasingly be used against malicious cyber actors, including non-state cybercriminals, this research can help guide a strategic approach for how to proceed.

The US government is using sanctions more than ever before (Gilsan, 2019) [15]. According to the GAO, there are now 20 country-based sanctions programs. Additional programs target individuals or entities regardless of their geographic location for their involvement in security threats like terrorism, narcotics trafficking, and malicious cyber

activity (US Government Accountability Office, 2019). Even as more sanctions are imposed, and foreign governments adopt their own measures, however, assessing the effectiveness of these actions remains a difficult process. GAO found that may be, in part, because US government entities are not required to determine whether sanctions "work" (US Government Accountability Office, 2019). In October 2019, GAO reported that the Departments of Treasury, State, and Commerce conduct assessments on sanctions' impact on specific targets, but not their overall effectiveness in meeting US policy goals (US Government Accountability Office, 2019).

Sanctions research sheds light on when these measures overall can be most effective. The US Cyberspace Solarium Commission rightfully highlighted in its final report that the "efficacy of sanctions depends heavily on a number of factors, including their target and timeline, the degree of international coordination, and the path to lifting them" (US Cyberspace Solarium Commission, 2020). Some research has suggested that economic sanctions have resulted in some meaningful change in the sanctioned country about 40% of the time (Peksen, 2019) [33]. However, scholars debate whether there is an actual causal relationship between sanctions and these behavioral changes in a number of cases. For example, some see South Africa's repeal of the legal framework for apartheid as a direct result of sanctions. Others maintain it was unrelated (Levy, 1999). Libya's decision to abandon its weapons of mass destruction programs and support for terrorism in 2003 has been held as a model for an effective sanctions regime, but others question whether other issues and actions had a greater influence on this decision (Nephew, 2018) [30].

Against state actors, sanctions have proved effective when implemented multilaterally, effectively messaged, and as part of a coherent strategy. GAO found that sanctions were successful in changing behaviour when they were implemented in concert with other countries and "when targeted countries had some existing dependency on or relationship with the United States," such as foreign aid or military support (US Government Accountability Office, 2019). GAO also found "strong evidence that the economic impact of sanctions has generally been greater when they were more comprehensive in scope or severity" (US Government Accountability Office, 2019). But there is also evidence to suggest that when sanctions are effectively messaged (i.e., when the sanctioned state understands what behaviour the sanctions are targeting and what behaviour is necessary to achieve a lifting in sanctions) sanctioned states are more likely to change their behaviour (Mortlock & Brian 2018) [8].

Research on sanctions against non-state actors has focused primarily on their impact on terrorism (Rosenberg, *et al*., 2016) [37]. The studies find that sanctions are not particularly effective at changing terrorists' ideology but can effectively disrupt their access to financial markets, thereby limiting their ability to conduct attacks (Zarate, 2013) [49]. The application of national and international sanctions, coupled with close cooperation with foreign partners and the private sector, and enhancements in international financial transparency have made it harder for "terrorist groups to raise, move, store, and use funds" (US Department of the Treasury, 2014). In particular, al-Qaeda's financial network has been undermined through the use of targeted financial measures, sustained engagement in key areas, and the development of innovative systems by which to collect financial intelligence" (US Department of the Treasury, 2014). Inthepost-9/11period, scholars have noted the success of the international community in "significantly hobbling terrorist groups by restricting access to legitimate financial channels" (The Council on Foreign Relations, 2011). Disrupting these sources has been a core component of the fight to destroy terrorist groups (US Department of State, 2014) and could be similarly successful against transnational criminal organizations that rely on cybercrime for resources.

Implications of this research on cyber-related sanctions

Lessons learned from this research indicate that coordinating cyber sanctions with foreign partners and the private sector and quickly identifying and seizing financial assets is essential when dealing with non-state cybercriminals. Cybercriminals with no ties to nation-states may have fewer links to the global financial system, which may mean targeted sanctions could be effective against these actors though they have been rarely used against them (Zarate, 2013) [49]. This research also suggests effectively messaging what behaviour the sanctions are targeting and what can be done by the targeted actor to reduce those sanctions may deter future cybercrime (Rosenberg & Jordan, 2019).

However, the imposition of sanctions can have drawbacks. First, over time, international compliance with sanctions can diminish, particularly when the sanctioned activity has passed (Haas, 1998) [2]. Second, too many sanctions may limit the potency of sanctions in the future. Banks are subject to liability if they maintain accounts for illicit actors, even if they did not will fully violate sanctions regimes (Saperstein & Geoffrey, 2015) [38]. To avoid incurring stiff penalties, they will often not open accounts with respect to certain activities (McKendry, 2014). Additionally, legitimate entities and people may seek out alternative financial systems to avoid liability concerns, driving them away from the US financial system. This may include the increased use of cryptocurrency (Myers *et al*., 2020) [29]. Paradoxically, this limits the reach of US sanctioning power by driving illicit activity to unregulated areas and pushing higher-risk clients to banks that may have fewer resources to detect illegal transactions (McKendry, 2014). Finally, the overuse of sanctions may impugn the power of sanctions as a tool to advance US goals in the future if they do not result in the intended effect (Lowery, 2015) [27]. A continual reassessment of how cyber sanctions t into a broader strategic approach toward dealing with their targets and their impact is vital to mitigate these risks.

Nonetheless, sanctions can be a useful tool to impact a target's behaviour and impose consequences on those that may be out of reach for US law enforcement authorities. The US Cyberspace Solarium Commission found the use of sanctions as part of a layered deterrence strategy "will not eliminate state-sponsored cyber operations or cybercrime, but consistently enforced consequences and rewards can begin to erode the incentives for bad behaviour" (US Cyberspace Solarium Commission, 2020). Sanctions can also have other critical impacts such as cutting off financial flows, galvanizing global support for further actions against malicious cyber actors, and enforcing norms of responsible behavior in cyberspace. They may also serve an important signalling function by allowing the US government to detail

the malicious cyber activity it is targeting in the public domain. This could, for example, signal to cybersecurity practitioners those actors they should be particularly focused on (This could include providing important threat information to key cybersecurity companies such as those that are members of the Cyber Threat Alliance) (Cyber Threat Alliance, 2020). Moving forward, Congress must now exercise its oversight role over US cyber-related sanctions to assess their impact.

Conclusion

In recent years, sanctions have emerged as a frequent tool of American foreign policy. Since the cyber-related sanctions program was formally established, these sanctions have increasingly, albeit sparingly, been used as a tool to impose consequences on malicious cyber actors. Yet, there is little publicly available data to assess whether these cyber sanctions have had an impact in changing their target(s) behaviour or achieving other established goals. Research on sanctions broadly offers some guidance on how cyber sanctions can prove effective. Accounting for these insights, Congress should exercise its oversight function and raise a number of questions about the strategy and impact of cyber sanctions during budget and nomination hearings and meetings with the Executive Branch. This should include raising the question as to whether sanctions should be used more to target cybercriminals. Finally, Congress should push for a formal assessment on the impact of the US government's cyber sanctions program and provide support for organizations to conduct independent research into these questions.

Appendix 1

The following chart documents the sanctions that have been issued by the US government for malicious cyber activity under a number of authorities, including but not limited to the cyber- enabled sanctions program. It lists the country or non-state actor linked to the malicious cyber activity (though it should be noted that those listed as non-state actors may have some linkages to state entities), the number of individuals or entities sanctioned, the authority under which the sanctions were issued, and the date of issuance.

Table 1

Authority	Date
Terrorism (EO 13224)	2/16/12
Human Rights (EO 13606)	4/23/12
Iran Threat Reduction and Syrian Human Rights Act (P.L. 112-158)	2/6/13
Iran (EO 13628)	5/31/13
Iran (EO 13628), Human Rights (EO 13553)	12/30/14
Cyber (EO 13694)	9/14/17
Iran (EO 13606, 13628)	1/12/2018
Cyber (EO 13694)	3/23/18
Iran (EO 13606, 13628)	5/30/18
Iran (EO 13606)	2/13/19
Weapons of Mass Destruction (EO 13382)	3/22/19
Human Rights (EO 13553, 13572), Terrorism (EO 13224)	9/17/20
Election Interference (EO 13848)	10/22/20
Iran (EO 13628)	11/8/12
North Korea (EO 13687)	1/2/15
North Korea (EO 13722)	9/6/18
North Korea (EO 13722)	9/13/19
Cyber (EO 13757)	12/29/16
Cyber (EO 13694), CAATSA	3/15/18
Ukraine (EO 13661, 13662), Syria (EO 13582), CAATSA	4/6/18
Cyber (EO 13694), CAATSA	6/11/18
Cyber (EO 13694), CAATSA	8/21/18
Cyber (EO 13694), CAATSA	12/19/18
Election Interference (EO 13848)	9/30/19
Cyber (EO 13694), CAATSA	12/5/19
Cyber (EO 13694) Election Interference (EO 13848)	9/10/20
Election Interference (EO 13848), Cyber (EO 13694), Ukraine (EO 13661)	9/23/20

Table 2

CAATSA	10/23/20
Cyber (EO 13694)	12/29/16
Transnational Criminal Organizations (EO 13581)	7/18/17
Cyber (EO 13694)	11/28/18
Cyber (EO 13694)	3/2/20
Cyber (EO 13694)	6/16/20
Cyber (EO 13694)	7/15/20
Cyber (EO 13694, 13757)	9/16/20

This data is primarily drawn from "Countering Malicious Cyber Activity: Targeted Financial Sanctions" by Natalie Thompson. It has been reorganized and brought up to date as of January 1, 2021. *See* Thompson, Natalie. "Countering Malicious Cyber Activity: Targeted Financial Sanctions." *Carnegie Endowment for International Peace*, Oct. 2020, p. 11-13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770816. Accessed 23 Jan. 2021.

References

1. Ablon Lillian. "Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data." Rand, Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, 2018.

www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf. Accessed 30 Nov. 2020.
2. Albert Eleanor. "What to Know About Sanctions on North Korea." *The Council on Foreign Relations*, 2019. https://www.cfr.org/backgrounder/what-know-about-sanctions- north-korea. Accessed 01 Dec. 2020. Haas, Richard. "Economic Sanctions: Too Much of a Bad Thing." *Brookings Institute*, 1 June 1998, https://www.brookings.edu/research/economic-sanctions-too-much-of-a-bad-thing/. Accessed 30 Nov. 2020.
3. Bergal Jenni. "Cybercriminals StrikeSchools Amid Pandemic," *Pew*, 2020. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/09/22/cybercriminals-strike-schools-amid-pandemic. Accessed 28 Dec. 2020.
4. Botek Adam. "European Union establishes a sanction regime for cyber-attacks." *NATO Cooperative Cyber Defence Centre of Excellence*, ccdcoe.org/library/publications/european- union-establishes-a-sanction-regi me-for-cyber-attacks/. Accessed 28 Dec. 2020; "UK Cyber Sanctions," *UK.gov*, 18 June 2020, www.gov.uk/government/collections/uk-cyber-sanctions. Accessed 28 Dec. 2020.
5. Chain Analysis. "Crypto Crime Summarized: Scams and Darknet Markets Dominated 2020 by Revenue, But Ransomware Is the Bigger Story, 2021. https://blog.chainalysis.com/reports/2021-crypto-crime-report-intro-ransomware-scams-darknet-markets. Accessed 21 January 2021.
6. Countering America's Adversaries Through Sanctions Act of 2017, Public Law 115-44, U.S. Statutes at Large (2017), https://www.treasury.gov/resourcecenter/sanctions/Programs/Documents/hr3364_pl115-44.pdf. Accessed 28 Dec. 2020.
7. Cyentia Institute, "Information Risk Insight Study 20/20, Extreme, Analyzing the 100 largest cyber loss events of the last five years." 2020, pp. 23. https://www.cyentia.com/wp-content/uploads/IRIS2020-Xtreme.pdf. Accessed 28 Dec. 2020. *112shrg73840.htm. Accessed 30 Dec. 2020.*
8. David Mortlock, Brian O'Toole. "US sanctions: Using a coercive and economic tool effectively." *The Atlantic Council*, 2018. https://www.atlanticcouncil.org/in-depth- research-reports/issue-brief/us-sanctions-using-a-coercive-and-economic-tool-effectively/. Accessed 03 Nov. 2020.
9. EO 13694 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". 01 Apr. 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging- significant-m. Accessed 14 Jan. 2021.
10. EO 13757. "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities". 28 Dec. 2016, https://home.treasury.gov/system/files/126/cyber2_eo.pdf. Accessed 01 Dec. 2020.
11. EO 13848. "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election". 12 Sept 2019, https://www gpo gov/fdsys/pkg/FR-2018-09-14/pdf/2018-20203 pdf. Accessed 23 Jan. 2021.
12. Fernandez, Manny, *et al*. "Ransomware Attacks Hits 22 Texas Towns, Authorities Say." *The New York Times*, 20 Aug. 2019, www.nytimes.com/2019/08/20/us/texas-ransomware.html. Accessed 28 Dec. 2020
13. Fishman, Edward. "How to Fix America's Failing Sanctions Policy." *Lawfare*, 2020. https://www.lawfareblog.com/how-fix-americas-failing-sanctions-policy. Accessed 30 Nov. 2020.
14. Gibson Dunn. 2020 "2019 Year-End Sanctions Update.". https://www.gibsondunn.com/wp-content/uploads/2020/01/2019-year-end-sanctions-update.pdf. Accessed 28 Dec. 2020.
15. Gilsan Kathy. "A Boom Time for U.S. Sanctions." The Atlantic, 2019. https://www.theatlantic.com/politics/archive/2019/05/why-united-states-uses-sanctions- so-much/588625/. Accessed 30 Dec. 2020.
16. Glaser Daniel. Assistant Secretary for Terrorist Financing, U.S. Department of the Treasury, Statement to the Subcommittee on Crime and Terrorism, Committee on the Judiciary, U.S. Senate, 2011. https://www.govinfo.gov/content/pkg/CHRG-112shrg73840/html/CHRG-112shrg73840.htm. Accessed 30 Dec. 2020.
17. Goldsmith Jack, Williams Robert. "The Failure of the United States' Chinese-Hacking Indictment Strategy." Lawfare, 2018. https://www.lawfareblog.com/failure-united- states-chinese-hacking-indictment-strategy. Accessed 28 Dec. 2020.
18. Healey Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks" *The Atlantic Council*, 2012. www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF. Accessed 28 Dec. 2020.
19. Hufbauer Gary. "Sanctions Sometimes Succeed: But No All-Purpose Cure." *Cato Unbound*, 2014. https://www.cato-unbound.org/2014/11/07/gary-clyde-hufbauer/sanctions- sometimes-succeed-no-all-purpose-cure. Accessed 30 Nov. 2020.
20. Jeffrey Frankel. "The 1807-1809 Embargo of Britain,." *Journal of Economic History*,1982:42(2):291–308. https://doi.org/10.1017/S0022050700027443. Accessed 30 Nov. 2020.
21. Joint cybersecurity advisory coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS). "Ransomware Activity Targeting the Healthcare and Public Health Sector." https://us-cert.cisa.gov/sites/default/files/publications/AA20302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector. pdf. Accessed 28 Dec. 2020.
22. Jordan Joseph. "Sanctions were crucial to the Defeat of Apartheid." *The New York Times*, 2013. https://www.nytimes.com/roomfordebate/2013/11/19/sanctions-successes-and- failures/sanctions-were-crucial-to-the-defeat-of-apartheid. Accessed 01 Dec. 2020.
23. Lauren Frias. "Louisiana's governor declared a state of emergency after a cybersecurity attack on government servers." *Business Insider*, 2019. https://www.businessinsider.com/louisiana-declares-

state-of-emergency-after- cybersecurity-attack-2019-11. Accessed 30 Nov. 2020.
24. Lewis James, Smith Zhanna. "The Hidden Costs of Cybercrime," *Center for Strategic and International Studies*, 2020. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf. Accessed 28 Dec. 2020.
25. Logan Trevor. "Washington Uses Sanctions and Indictments Inconsistently When Combating Malicious Cyber Activity." *Foundation for Defense of Democracies*, 2020. https://www.fdd.org/analysis/2020/04/15/washington-uses-sanctions-and-indictments-inconsistently-when-combating-malicious-cyber-activity/. Accessed 28 Dec. 2020.
26. Lorber Eric, Schneider Jacquelyn. "Sanctioning to Deter: Implications for Cyberspace, Russia, and Beyond." *War on the Rocks*, 2015. https://warontherocks.com/2015/04/sanctioning-to-deter-implications-for-cyberspace-russia-and-beyond/. Accessed 30 Nov. 2020.
27. Lowery Clay, Ramachandran Vijaya. "Unintended Consequences of Anti-Money Laundering Policies for Poor Countries." Center for Global Development, 2015, 47. http://www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf. Accessed 14 Jan. 2021.
28. Mortlock David, O'Toole Brian. "US sanctions: using a coercive and economic tool effectively." The Atlantic Council, 2018. https://www.atlanticcouncil.org/in-depth- research-reports/issue-brief/us-sanctions-using-a-coercive-and-economic-tool-effectively/. Accessed 30 Dec. 2020.
29. Myers Adam, *et al*. "Crypto-controls: Harnessing Cryptocurrency to Strengthen Sanctions, 2020. https://warontherocks.com/2020/12/crypto-controls-harnessing-cryptocurrency- to-strengthen-sanctions/. Accessed 23 Jan. 2021.
30. Nephew Richard. "Libya: Sanctions Removal Done Right? A Review of The Libyan Sanctions Experience, 1980–2006, 2018. https://energypolicy.columbia.edu/sites/default/files/pictures/Libya%20Sanctions%20Removal_CGEP_Report_031918.pdf. Accessed 01 Dec. 2020.
31. Newman Lily Hay. "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare." *Wired*, 2018. https://www.wired.com/story/atlanta-spent-26m-recover-from- ransomware-scare/. Accessed 30 Dec. 2020.
32. Omar Ilhan. "Sanctions are part of a failed foreign policy playbook. Stop relying on them." *The Washington Post*, 2019. https://www.washingtonpost.com/opinions/ilhan-omar-sanctions-are-part-of-a-failed-foreign-policy-playbook-stop-relying-on-them/2019/10/23/b7cbb1ca-f510-11e9-a285-882a8e386a96_story.html. Accessed 30 Nov. 2020;
33. Peksen Dursun. "When do Economic Sanctions Work Best?" Center for a New American Security, 2019. https://www.cnas.org/publications/commentary/when-do-economic- sanctions-work-best. Accessed 30 Dec. 2020.
34. Peters Allison, Garcia Michael. "A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?." Third Way, 2020. https://www.thirdway.org/report/a- roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here.
35. President Barack Obama White House. "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." Executive Order, 1 Apr. 2015, https://obamawhitehouse.archives.gov/the-press-o ce/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m. Accessed 28 Dec. 2020.
36. Reinhart RJ. "One in Four Americans Have Experienced Cybercrime." *Gallup*, 2018. news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx. Accessed 30 Nov. 2020.
37. Rosenberg Elizabeth, Goldman Zachary, Drezner Daniel, Solomon Strauss Julia. "The New Tools of Economic Warfare, Effects and Effectiveness of Contemporary U.S. Financial Sanctions." Center for a New American Security, 2016, 28-32.
38. Saperstein Lanier, Sant Geoffrey. "Account Closed: How Bank 'De-Risking' Hurts Legitimate Customers." The Wall Street Journal, 2015. https://www.wsj.com/articles/account-closed-how-bank-de-risking-hurts-legitimate-customers-1439419093. Accessed 14 Jan. 2021.
39. The Council on Foreign Relations, "The Global Regime for Terrorism, 2011. https://www.cfr.org/report/global-regime-terrorism. Accessed 30 Dec. 2020
40. Thompson Natalie. "Countering Malicious Cyber Activity: Targeted Financial Sanctions" *Carnegie Endowment for International Peace*, 2020, 3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770816. Accessed 23 Jan. 2021.
41. United States, Congress. International Emergency Economic Powers Act (IEEPA). Congress.gov, https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter35&edition=prelim, 95 th Congress. Pub.L. 95–223, title II, §202, 91 Stat. 1626, passed Dec. 28, 1977. Accessed 01, Dec. 2020.
42. US Congress, 116 th Congress, https://www.congress.gov/bill/116th-congress/house-bill/1493?q=%7B%22search%22%3A%5B%22H. R. 3941%22%5D%7D. n and US Congress, 116 th Congress, https://www.congress.gov/bill/116th-congress/senate-bill/482/text.
43. US Department of Justice. "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research." 21 Jul. 2020, https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security- charged-global-computer-intrusion. Accessed 14 Jan. 2021.
44. US Department of Treasury. "Consolidated Sanctions List Data Files." 14 Dec. 2020, https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-data-files. Accessed 28 Dec. 2020.
45. US Department of Treasury. "Treasury Targets Financier's Illicit Sanctions Evasion Activity." 15 Jul. 2020, https://home.treasury.gov/news/press-releases/sm1058. Accessed 14 Jan. 2021.

46. US Government Accountability Office. “Economic Sanctions: Agencies Assess Impacts on Targets, and Studies Suggest Several Factors Contribute to Sanctions' Effectiveness.” 2 Oct. 2019, www.gao.gov/products/GAO-20-145. Accessed 30 Nov. 2020.
47. US White House, The Council of Economic Advisers. *The Cost of Malicious Cyber Activity to the U.S. Economy*. February 2018, p. 36. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 28 Dec. 2020.
48. White House. “FACT SHEET: President Xi Jinping’s State Visit to the United States”. 25 Sept. 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet- president-xi-jinpings-state-visit-united-states. Accessed 29 Dec. 2020.
49. Zarate Juan. Treasury’s War: The Unleashing of a New Era of Financial Warfare. (New York: Public Affairs, 2013).