NOWHERE TO HIDE: INVESTIGATING THE USE OF UNILATERAL ALTERNATIVES TO EXTRADITION IN UNITED STATES PROSECUTIONS OF TRANSNATIONAL CYBERCRIME

Christopher J. D'Urso
St John's College

Thesis submitted in partial fulfillment of the requirements of the degree of DPhil in Public Policy at the Blavatnik School of Government at the University of Oxford

TRINITY TERM 2021

Word Count: 92,560

TABLE OF CONTENTS

ABSTRACT

Transnational cybercrime is an increasing public menace, and prosecuting countries must often turn to extradition and its alternatives to bring perpetrators to justice. These alternatives include quasi-extradition (informal cooperation with the host country) and unilateral action (capture or lure operations). I posit that pursuing countries are more likely to employ unilateral alternatives over extradition and quasi-extradition in prosecutions of cybercrime as compared to other transnational crimes. I predict this is due to the remote nature of cybercrime; legal barriers; and political considerations in the host country.

The United States is a leader in prosecuting cross-border cybercrime, so I focus my analysis there. Interviews with 81 US officials and case studies suggest that unilateral alternatives are applied more frequently for cybercrime. I uncover that the need for such tools does not stem from legal barriers. Rather, it stems from the remote and anonymous nature of cybercrime, a lack of political will in host countries, and state sponsorship.

I then compare the trajectory of transnational cybercrime prosecutions to those of terrorism; drug trafficking; fraud and foreign corruption; and export control and sanctions violations. Unlike these other offenses, I conclude that cybercrime prosecutions cannot be expected to rely, even in the long-term, on cooperation with the host country or the perpetrators traveling as part of the conspiracy. This foreshadows that cybercrime prosecutions will likely require a sustained reliance on unilateralism.

Building on existing scholarship related to the use of unilateral alternatives in war crimes, terrorism, and drug trafficking prosecutions, I thus propose a pragmatic framework to guide pursuing countries when the use of lures may be prudent in cybercrime cases. This framework seeks to mitigate any infringements on the sovereignty of the host country and human rights of the accused while still enabling the pursuing country to end ongoing cybercrimes, recognize victims' injuries, and deter future attacks.

ACKNOWLEDGEMENTS

First and foremost, I would not be where I am without the love, support, and encouragement of my parents. You always believed in me and inspired me to shoot for the stars. No matter how crazy or ambitious my goals, you gave up countless hours to help me achieve those dreams. Above all, you instilled in me the values of hard work, integrity, and humility that have shaped me into the person I am today and that will forever guide me.

I could not have completed this DPhil without the wise advice and guidance of my supervisor, Professor Karthik Ramanna. There are no words to adequately thank you for the incredible amount of time and energy you dedicated to my research. You challenged me at every step to think big and develop an ambitious dissertation with real-world policy relevance. You taught me how to formulate water-tight arguments while still maintaining an engaging, narrative writing style. I simply could not have asked for a better supervisor.

This dissertation would also not have been possible without the law enforcement officials who kindly agreed to speak with me and share their insights and experiences in an area that is often hidden from the public view.

Additionally, I would like to thank my friends at Oxford, particularly my DPhil colleagues, for providing a sounding block for my ideas and volunteering to offer feedback on draft chapters. You helped me to work through the many difficult research and policy questions I encountered. On a personal level, I know that I will cherish the friendships and countless memories formed here for many years to come.

Furthermore, I would like to express my sincere gratitude to Professors Dapo Akande and Joss Wright for serving as my Transfer of Status and Confirmation of Status assessors and providing such helpful feedback on my research proposal, literature review, Chapter 4, and Chapter 5. Likewise, I would like to thank Professor Miles Jackson of the Oxford Law Faculty as well as Federica D'Alessandra and Dr Elizabeth Stubbins Bates of the Oxford Institute of Ethics, Law and Armed Conflict for sharing their thoughts on Chapter 6, particularly my framework on the use of unilateral lure operations.

I would be remiss if I did not acknowledge the Rhodes Trust for affording me the life-changing opportunity to study at Oxford. These past three years not only facilitated my academic development but also enabled me to grow as person and aspiring public servant. I would like to extend a special thank you to Mary Eaton, Registrar and Director of Scholar Affairs at the Rhodes Trust, for convincing me to pursue a DPhil and offering unwavering support along the way.

St John's College and the Blavatnik School of Government also contributed essential funding for my research, particularly my fieldwork in the United States.

Finally, I would like to thank Dean Heather Gerken of Yale Law School and LexisNexis for providing me with access to key US legal research resources that were not available at Oxford. Similarly, the University of Pennsylvania Biddle Law Library and Leadership Connect granted me access to the Federal Yellow Book, which was an invaluable tool in identifying and locating contact information for potential interviewees.

TABLE OF ABBREVIATIONS

AAG	Assistant Attorney General
AUSA	Assistant United States Attorney
CCIPS	Computer Crime and Intellectual Property Section
CoE	Council of Europe
CUREC	Central University Research Ethics Committee
DAAG	Deputy Assistant Attorney General
DAG	Deputy Attorney General
DEA	Drug Enforcement Administration
FBI	Federal Bureau of Investigation
FCPA	Foreign Corrupt Practices Act
FSB	Federal Security Service of the Russian Federation
FRY	Federal Republic of Yugoslavia
G20	Group of 20
GRU	Russian Main Intelligence Directorate
HSI	Homeland Security Investigations
ICC	International Criminal Court
ICCPR	International Covenant on Civil and Political Rights
ICTY	International Criminal Tribunal for the Former Yugoslavia
ILC	International Law Commission
IP	Intellectual Property
ISIS	Islamic State of Iraq and Syria
LCO	Lure and Capture Operation
NATO	North Atlantic Treaty Organization
NSD	National Security Division

OIA	Office of International Affairs
PAW	Provisional Arrest Warrant
PII	Personally Identifiable Information
PLA	Chinese People's Liberation Army
SDO	Seizure and Delivery Operation
TCL	Transnational Criminal Law
UN	United Nations
UNODC	UN Office on Drugs and Crime
UNTOC	UN Convention against Transnational Organized Crime
USDOJ	US Department of Justice

1. INTRODUCTION

It was Friday, May 30, 2014. Law enforcement officials and cybersecurity researchers around the world readied for battle. This was the first time that all the key stakeholders had finally joined together to take down the Gameover Zeus botnet. Gameover Zeus was a pernicious form of malware that relied on familiar techniques. It was circulated via unsolicited emails with malicious links. The joke, within the cybersecurity community, was that once a victim clicked on the link and infected their devices, "it was game over for your bank accounts."[1]

Not only would the malware begin siphoning your bank accounts. It would also deploy the army of infected computers that it had amassed to target your bank with a massive denial of service attack. The goal: to distract bank employees and customers from noticing that any money was missing until the transfer cleared.[2] The US Federal Bureau of Investigation (FBI) estimates that this scheme cost over $100 million alone.[3]

However, the perpetrators were not done. They recognized that the majority of compromised computers did not belong to individuals or organizations with large bank accounts. So, the cybercriminals began deploying a new form of ransomware called CryptoLocker against those idle devices. CryptoLocker would lock all the victims' files until they paid a few hundred dollars. The ransoms were kept small to discourage victims from reporting these crimes to the police. As one cybersecurity researcher recalled, the CryptoLocker business model "'created a new type of online crime.'"[4]

The problem with Gameover Zeus was that it "was designed from the start to be takedown-proof."[5] It relied on both command servers and peer-to-peer communication.

---

[1] Carlin, *Dawn of the Code War*, 290.
[2] Carlin, 291.
[3] "U.S. Leads Multi-National Action Against 'Gameover Zeus' Botnet and 'Cryptolocker' Ransomware, Charges Botnet Administrator."
[4] Quoted in Carlin, *Dawn of the Code War*, 292.
[5] Carlin, 290.

This means that the minute a command server was taken down, the other computers in the botnet would rely on the peer-to-peer network to find another command server.

When law enforcement finally prepared to bring down Gameover Zeus, they knew they were in for a fight. Indeed, within hours, the man they had identified as the leader of this conspiracy, Evgeniy Mikhailovich Bogachev, was "wrestling for control of his network."[6] The former United States Attorney overseeing the case described the take-down as "'cyber-hand-to-hand combat.'"[7] Sixty hours later, the team of law enforcement and cybersecurity researchers had won. Gameover Zeus was dead.

Yet, celebration would be premature. Bogachev remains at large. During the investigation, law enforcement discovered that he was not only using the botnet to steal banking information. He was also using it to search for information related to Georgian intelligence officers and the leaders of Turkish police units as well as classified material on the conflict in Syria and Russian arms deals. In fact, just as Russian forces invaded the Crimea, Bogachev was searching Ukrainian computers for any information that could assist Russia in the conflict. While law enforcement could not find a specific link between Bogachev and the Russian government, former Assistant Attorney General for the US Department of Justice's (USDOJ) National Security Division John Carlin claims, "Bogachev, it appeared, was a Russian intelligence asset."[8]

As a result, Bogachev is suspected to be in Russia where he remains able to launch new and potentially even more devastating cyberattacks against victims around the world. It's possible that he's done so already and that victims have not yet reported it or law enforcement has not yet linked new forms of malware to him. Unfortunately, Bogachev is

[6] Carlin, 300.
[7] Quoted in Carlin, 301.
[8] Carlin, 297.

not the only cybercriminal to escape justice. Based on data from the FBI, the think tank Third Way has estimated that only 3 out of every 1,000 cyber incidents result in arrest.[9]

This enforcement gap is particularly disconcerting considering the scale and growth of cybercrime. In 2015, the damages from cybercrime around the world cost $3 trillion. By the end of 2021, that figure is expected to double to $6 trillion. If that figure represented the GDP of a country, it would be the world's third-largest economy. That estimate also means cybercrime is likely to cost the world $11.4 million every minute.[10]

Cybercrime poses special challenges for law enforcement since perpetrators are frequently located in another country from their victims or route their offenses through multiple countries.[11] Given that no country can combat this problem alone, countries pursuing transnational cybercriminals must seemingly rely upon international coordination to bring these individuals to justice.[12]

This cooperation is necessary at two main stages. First is to secure the evidence to identify the perpetrator and establish guilt beyond a reasonable doubt. Second is to secure custody over the offender for prosecution in the pursuing country's domestic courts. This dissertation focuses on that second component.

The traditional legal approach to such international cooperation is extradition. However, extradition has historically faced political and procedural challenges that impede its effectiveness. As a result, pursuing countries may need to contemplate alternative approaches to lay their hands on the defendant. This study seeks to shed light on how the challenges of securing custody over the perpetrator unfold in cybercrime

[9] Eoyang et al., "To Catch a Hacker."
[10] Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025."
[11] Verdelho, "The Effectiveness of International Co-Operation against Cybercrime: Examples of Good Practice," 4.
[12] Bringing to justice refers to "a law enforcement action with the end result of: (i) prosecuting an individual for a charged crime; or (ii) punishing an individual whose guilt has been established but has yet to pay his debt to society, whether by incarceration, re-incarceration (in the event of a prison escape), or other legally sanctioned means." Sadoff, *Bringing International Fugitives to Justice*, 3.

cases. It also explores how countries deploy alternatives to extradition to bring international cybercriminals to justice. Specifically, I ask the following research questions:

1. *Are pursuing countries more likely to apply unilateral alternatives over extradition and quasi-extradition in prosecutions of cybercrime than other transnational crimes?*
2. *What factors influence the use of unilateral alternatives to extradition in cybercrime cases?*

In this introductory chapter, I define the key terms that are used throughout the study. I then preview the existing debates in the literature that motivate these research questions and briefly outline the research methodology. I conclude the chapter with a discussion of this dissertation's contributions and policy implications as well as a roadmap for the remainder of the thesis.

1.1 Definitions of Key Terms

Pursuing country refers to the country that is seeking to secure custody over an offender in order to prosecute that individual in their domestic criminal courts.[13]

Host country refers to the country where the defendant is located, regardless of how temporarily he is in that jurisdiction. For example, if a defendant resides in country A but voluntarily travels to country B, country B would become the host country for as long as the defendant remains in that territory.

Extradition refers to the formal legal process whereby one country renders an individual who has been accused of a crime in another country to stand trial there or to

[13] The term pursuing country is used in lieu of alternative phraseology such as requesting country or forum country since there may not always be a formal extradition request and the country in question may not always be successful in bringing the defendant before their courts. Rather, the term pursuing country clearly delineates the relationship between the country and fugitive, regardless of the process used or ultimate success. For a further discussion, see Sadoff, 34–36.

serve a sentence that has already been determined in that country. This process is typically governed by a treaty between the pursuing country and host country.

Alternatives to extradition, according to Sadoff, refer to "all measures, methods, and mechanisms, whether ultimately regarded as lawful or unlawful, that: (i) fall outside the extradition regime; (ii) aim to bring a fugitive to justice fully or partially, directly or indirectly; and (iii) do not entail a fugitive's delivery as a function of sheer fortuity."[14] This dissertation solely focuses on those alternatives to extradition that intend to fully and directly bring a criminal to justice through the pursuing country's courts. It does not consider mechanisms that attempt to hold perpetrators accountable outside of the pursuing country's justice system. For the purposes of this analysis, there are two types of alternatives to extradition: quasi-extradition and unilateral alternatives.

Quasi-extradition occurs when the host country cooperates in rendering the fugitive outside of the formal extradition process, such as by using immigration laws to deport the fugitive or informally handing him over.

Unilateral alternatives to extradition refer to when the pursuing country seeks to secure custody over the fugitive outside of the formal extradition process and without the involvement of the host country or the host country's agents acting in their official capacity. This may occur via luring, kidnapping, or interception. It is important to note that a third country may be involved in the unilateral alternative by, for example, serving as the lure destination. However, it is still considered a unilateral alternative for the purposes of this analysis as long as the host country is not involved in the rendition.

Cybercrime refers to crimes which target computer systems or information technology as well as those where information technology is essential to the commission of the illicit conduct. This definition includes all crimes where the cyber element plays a

[14] Sadoff, 605.

key role and that may therefore experience similar challenges to securing custody. However, it does not incorporate offenses where the cyber element is not essential. Given that virtually all crimes now involve technology or electronic evidence in some way, a broader definition would risk including conduct that is no different than its real-world equivalent, particularly with respect to the prospects for laying hands on the accused.

Transnational crime refers to crimes that are committed in more than one state, in one state but with a significant portion of the preparation or control occurring in another state, in one state but involving organized criminal groups that operate in more than one state, or in one state but with significant effects in another state.[15] Examples include terrorism, drug trafficking, cross-border fraud, foreign corruption, and export control and sanctions violations.

1.2 Framing the Existing Debates in the Literature

The history of extradition can be traced as far back as 1280 BC when Ramses II of Egypt negotiated such an agreement with the Hittite prince Hattusili III. Much has changed with respect to extradition since that early treaty, which focused on rendering political opponents rather than ordinary criminals.[16] However, this rich history has provided ample opportunity for scholarship on the extradition regime and its effectiveness.

Existing studies have focused on the political and procedural challenges that have plagued extradition agreements. For instance, there is no international legal obligation for states to extradite fugitives unless they are party to a specific treaty. So, countries may refuse to sign such agreements based on their strategic interests. Additionally, extradition treaties require that the crime be illegal in both states, usually mandate that the pursuing

[15] This definition is derived from the United Nations Convention on Transnational Organized Crime (UNTOC). Although the UNTOC was written with respect to organized crime, it offers a general definition of transnational crime and is thus still suitable for this analysis. This definition is used since it enjoys widespread agreement whereby 190 countries are parties to the UNTOC.
[16] McDermott, "The Structure of International Cooperation in the Transfer of Suspects. Extradite or Abduct?," 258.

country satisfy onerous evidentiary requirements, and often prohibit the host country from extraditing their nationals.

Consequently, countries have sought to create a system of transnational criminal law to overcome these hurdles. They have drafted international conventions to harmonize legislation on certain types of crime and promote mutual legal assistance. Nevertheless, many of the same challenges persist. Host countries face no legal obligation to join such conventions. This means that their national laws may still fail to satisfy dual criminality requirements. Plus, they can continue refusing to hand over perpetrators.

Pursuing countries then face a quandary. Do they abandon the case or turn to an alternative approach? Quasi-extradition, like extradition, depends on the cooperation of the host country. As a result, the effectiveness of this alternative may be undermined by political barriers as well. Pursuing countries may therefore be left with unilateral alternatives, such as a lure or capture operation.

Much of the literature regarding those tools focuses on their permissibility under domestic and international law. While unilateral alternatives have been upheld by US courts, their international legality remains in question. Some scholars contend they violate territorial sovereignty,[17] human rights protections,[18] and prohibitions on the use of force.[19] In contrast, other scholars dispute these assertions. They claim that unilateral alternatives do not breach the sovereignty of the host country or the prohibition on the use of force. After all, they are directed at individuals rather than the host country's territorial integrity

[17] Sadoff, *Bringing International Fugitives to Justice*, 506, 510–16.
[18] Bassiouni, *International Extradition: United States Law and Practice*, 54–56.
[19] Sadoff, *Bringing International Fugitives to Justice*, 522–23.

or political independence.[20] Likewise, certain scholars contend that unilateral alternatives do not constitute arbitrary arrests since they are based on a lawful warrant or indictment.[21]

Despite these long-standing debates, significant gaps remain in the literature, which motivate this dissertation's core research questions. Primarily, there have been no attempts to examine the specific obstacles to extradition in cybercrime cases and the methods employed to secure custody over such offenders. Since the advent of cybercrime, academics have pondered whether it is a new form of criminality with unique features. Or is it merely a form of old wine in new bottles and "basically the same as the terrestrial crime with which we are familiar?"[22] This dissertation seeks to explore that question with respect to the prospects for laying hands on cybercriminals located abroad. This leads to the first research question:

1. *Are pursuing countries more likely to apply unilateral alternatives over extradition and quasi-extradition in prosecutions of cybercrime than other transnational crimes?*

The literature suggests that countries will apply unilateral alternatives as an infrequent last resort due to their potential to undermine diplomatic relations and respect for the rule of law. However, I contend that cybercrime is a unique form of transnational crime that alters state behavior.[23] I propose the following arguments as to how the distinct characteristics of cybercrime related to the facts of the case, applicable laws, and political considerations increase the likelihood that countries pursue unilateral action.

[20] Gurulé, "Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad," 486; Sadoff, *Bringing International Fugitives to Justice*, 505.
[21] Kallenbach, "Plomo O Plata: Irregular Rendition as a Means of Gaining Jurisdiction over Colombian Drug Kingpins," 212–13.
[22] Grabosky, "Virtual Criminality: Old Wine in New Bottles?," 243.
[23] Sadoff, *Bringing International Fugitives to Justice*, 588–90.

Due to the lack of physical constraints in cyberspace, the perpetrator is less likely to enter the victim country's territory.[24] This means the victim country cannot simply wait to arrest him within their borders. They must rely more heavily on extradition and its alternatives. Additionally, automation technologies and the lack of physical constraints allow cybercriminals to target victims in multiple countries at once.[25]

Consequently, multiple countries may claim jurisdiction over the same cybercriminal. Yet, there are no set criteria to prioritize such requests. It is also difficult to agree on the degree of harm across countries. This thereby diffuses the host country's incentives to support a given pursuing country's request.[26] Pursuing countries may then turn to unilateralism to preempt each other in securing custody over the offender.

Moreover, I predict the lack of legal harmonization on cybercrime creates a higher barrier to extradition. The conduct must be illegal in both the pursuing and host countries for extradition to proceed. However, I posit that many countries have not enacted adequate domestic legislation to outlaw cybercrime, requiring pursuing countries to apply alternative approaches. Extradition may also be less likely to succeed in cybercrime than other transnational crimes due to the political offense exception. As cybercriminals increasingly operate under the auspices or direction of state sponsors, they may claim that their conduct is simply a form of espionage and thus precluded from extradition.

Likewise, I assert that the lack of international consensus on cybercrime decreases the probability that host countries will cooperate through extradition and quasi-extradition. Plus, the victim is harder to empathize with since they are often located far away from the host country. Host countries would rather focus their limited law enforcement resources

[24] Brenner, "Distributed Security: A New Model of Law Enforcement."
[25] Brenner, 10.
[26] Clough, *Principles of Cybercrime*, 485.

on offenses that affect their citizens.[27] This thereby diminishes their interest in prosecuting domestically, extraditing, or cooperating through a quasi-extradition. The host country may also indirectly benefit from or actively sponsor cybercrime, which again precludes quasi-extradition. Pursuing countries, I contend, are then more frequently left with unilateral alternatives as their only option to bring the cybercriminal to justice.

These complications related to the facts of the case, applicable laws, and political considerations collectively lead me to the following hypothesis that:

Pursuing countries are more likely to employ unilateral alternatives over extradition and quasi-extradition in prosecutions of cybercrime than other transnational crimes.

Another gap in the literature is that there have been no empirical examinations, to my knowledge, of why countries deploy unilateral alternatives to extradition. Such an investigation can help shed light on what legal and policy improvements may be necessary to mitigate the need for unilateralism and promote international cooperation. This leads to the second research question:

2. *What factors influence the use of unilateral alternatives to extradition in cybercrime cases?*

Furthermore, while there have been attempts in the legal literature to identify when the use of unilateralism may be permissible for other types of crime, such efforts do not yet exist for cybercrime. Thus, understanding why states resort to unilateralism may also help determine when such alternatives may be prudent or justified in cyber cases.

[27] Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?," 472.

1.3 Research Design and Methodology

This study focuses on US efforts to bring international cybercriminals to justice. The US has adopted a leading role in the prosecution of cross-border cybercrime due to its superior expertise and experience. Since its actions drive global law enforcement action in this space, it is particularly interesting to study from a research perspective.

Nevertheless, this raises legitimate concerns that the results may not be generalizable beyond the US context. Indeed, the US enjoys a unique position as a global superpower. Testing my hypothesis involves a cross-sectional comparison between cybercrime and other transnational crimes within the US, which controls for the effects of the US's unique position. However, it is possible that the fear of meaningful retaliation is sufficiently low in the US to permit unilateral action. Yet, such fear may be much higher in other countries, causing them to eschew such methods.

As a result, I explore the generalizability of my findings by interviewing ten officials from eight other countries. The goal was to determine whether other countries experience the same challenges in securing custody over cybercriminals and deploy unilateral alternatives similarly to the US or not. The results of those conversations are reported throughout the dissertation, and I reflect further on the generalizability of my findings in the Conclusion chapter.

Overall, this study relies on a qualitative research design. In an ideal world, quantitative methods would likely be better suited to explore the first research question. A data set could be compiled including all US prosecutions of transnational crime and the methods used to secure custody over the perpetrators. I could then run a regression analysis to compare the usage of unilateral alternatives between cybercrime and other cross-border offenses. However, the US does not maintain data on how defendants were

rendered into its jurisdiction. As is further explained in Chapter 3, such information cannot be reliably gleaned from press releases either.

Therefore, this dissertation instead heard directly from the law enforcement officials responsible for prosecuting transnational crimes and deploying unilateral alternatives. In fact, a qualitative research approach presented several advantages, which were particularly helpful in studying an area like cybercrime that lacks well-developed theory. Primarily, this approach enabled me to engage in both theory testing and theory development, identifying new potential causal variables of interest. It also provided the rich, thick descriptions that elucidate the "why" behind relationships and cannot be provided by quantitative analysis alone. Such explanations were important for answering the second research question.

Specifically, this dissertation employed a combination of comparative elite interviews and case studies. The interviews focused on US federal prosecutors in leadership positions at the USDOJ headquarters in Washington, DC. These individuals oversee prosecutions of multiple crime areas across the country. Thus, they could offer the most holistic comparisons between types of transnational crime. I also spoke with federal prosecutors in the USDOJ field offices known as US Attorney's Offices and the leadership of the main investigating agencies to triangulate the responses. In total, I interviewed 81 US law enforcement officials. These conversations explored the challenges of securing custody over transnational criminals, the use of extradition and its alternatives, and the differences between cybercrime and other cross-border offenses. Interviewees were encouraged to answer these questions through the lens of specific cases on which they worked.

The case studies served as a further form of theory testing and theory development. They sought to determine which, if any, of the causal variables identified in the

comparative interviews played out in US cybercrime prosecutions involving unilateral alternatives. They also sought to detect any new causal variables of interest. The case studies employed the technique of process-tracing to explore the causal chains that led to a given outcome (the use of a unilateral alternative). This involved interviewing the specific prosecutors and federal agents who worked on the case. I also triangulated their responses with court records (e.g., indictments, sentencing memoranda, etc.) and media reporting to rule out alternative explanations. In total, I gathered sufficient information to conduct case studies of six cybercrime prosecutions involving unilateral alternatives.

Although this type of qualitative evidence has strengths, it is constrained by human memory and potential biases in the interviewees. For example, officials may struggle to accurately compare between types of crime over long periods of time. This means that the evidence is suggestive rather than dispositive. Additionally, they may seek to portray their actions or the US's efforts in the best light.

I attempted to mitigate these risks by interviewing a large number of officials and comparing responses between them. When I found that responses were largely consistent between interviewees and repeated by multiple officials, this provided me with greater confidence in the finding. When I found that responses contradicted each other or that only a few officials raised a given point, this generally limited the confidence with which I could make a claim. I also sought to address concerns regarding the bias of my US interviewees by speaking with officials from other countries.

1.4 Contributions and Policy Implications

This research contributes to our understanding of both cybercrime and the use of extradition and its alternatives. Many previous studies have examined the technical aspects of cybercrime as well as the challenges of international cooperation with respect to evidence-gathering and sharing across borders. However, there have been no such

investigation, to my knowledge, related to the methods used to secure custody over international cybercriminals.

Likewise, the existing research on extradition and its alternatives has focused on examining both domestic and international court precedent. This approach is useful for understanding how domestic and international law have evolved over time here. Nevertheless, there have been no on-the-ground attempts to understand how such tools are deployed in the many cases that do not make it into the law books. Indeed, focusing only on the cases that generate court precedent may lead to a biased understanding of alternatives to extradition since those prosecutions may be systematically different. For example, only cases involving abuses egregious enough or defendants notorious enough may warrant substantial appeals. Additionally, studying the court precedent alone cannot reveal why unilateral alternatives were deployed. Such internal law enforcement deliberations can only be ascertained by speaking directly with the officials involved.

Understanding the why is particularly important from a public policy perspective. On the one hand, unilateral alternatives are a vital tool to bring international fugitives to justice when all other remedies fail. They enable victims to receive their day in court and be vindicated. With respect to cybercrime, removing the perpetrator not only prevents him from launching future attacks. It also immediately ends any ongoing cybercrimes and stems the bleeding for victims. Furthermore, unilateral alternatives may raise the cost of cybercriminal conduct by increasing the likelihood of arrest and thus the risk of engaging in such illicit behavior. This means that such tools serve as a general deterrent as well.

However, there may be costs to unilateral alternatives. If the use of these tools breaches international law, Sadoff contends that this "undercut[s] the long, hard work it has taken to lay those foundations and to create a stable, predictable, and trust-based system for inter-State relations … The more States that act without regard to the law and

choose to circumvent it, the fewer remain with any credibility to insist on its proper operation."[28] Likewise, the use of unilateral alternatives may encourage the host country to engage in retribution against the pursuing country's citizens or other forms of retaliation.

Moreover, the use of unilateral alternatives may undermine faith in the utility of the extradition system. Despite its imperfections, the extradition regime facilitates the resolution of many cross-border criminal cases every year. Such an erosion of confidence may also weaken international law enforcement cooperation more generally. These relationships are crucial for securing evidence across borders, especially in today's digital age with data stored in all corners of the globe. Sadoff explains that the use of unilateral alternatives may sow distrust "in terms of the utility of existing treaties and procedures, as well as the need to negotiate new treaties or bring into force those that have been signed but not yet ratified."[29]

But, how can it be helpful to understand why unilateral tools are deployed? Primarily, it can enable us to craft recommendations on how to improve international law and policy to eliminate the root causes. Such changes would then mitigate the need for pursuing countries to apply unilateral tools. For example, if this study were to determine that dual criminality barriers account for the use of unilateral alternatives, it would suggest that greater attention be dedicated to harmonizing cybercrime legislation around the world. The less frequently that unilateral methods are required to secure custody, the less risk such actions pose of disrespecting international law, generating retaliation, and undermining the extradition regime.

[28] Sadoff, *Bringing International Fugitives to Justice*, 588.
[29] Sadoff, 589–90.

Nevertheless, the interplay of politics with extradition means that it will likely not be possible to fully eliminate the need for unilateralism. As a result, this dissertation also proposes a framework to outline baseline standards when the use of unilateral lure operations may be prudent in cybercrime cases.[30] This framework is informed by international law and existing justifications for unilateralism to combat other offenses. However, it does not seek to settle longstanding debates in international law on unilateralism. It rather serves as a pragmatic public policy guide for pursuing countries to consider when their lures are likely to provoke criticism, either from human rights or international law advocates.

The framework does not seek to limit or prohibit action that may be otherwise consistent with international law. It is instead a set of voluntary, non-binding norms that could be used to assess the advisability of unilateralism in cybercrime cases. Thus, if countries choose to go outside framework, such actions are not necessarily impermissible or unlawful. It simply means the use of the lure entails a greater risk of backlash from elements of the international legal and political community.

Overall, the framework provides pursuing countries with an avenue to bring cybercriminals to justice when international cooperation fails. This can help stop ongoing cyberattacks, deter future illicit conduct, and begin bridging the cyber enforcement gap. At the same time, following the framework assists countries in minimizing any intrusions on the sovereignty of host countries and human rights of the accused.

1.5 Dissertation Roadmap

This dissertation proceeds according to the following structure. In Chapter 2, I provide a more comprehensive review of the existing literature on extradition and its

[30] As will be reported in Chapter 4, lure operations are the only form of unilateral alternative deployed to combat transnational cybercrime. The threat is currently not considered significant enough to warrant a capture operation. Therefore, my findings on the second research question and correspondingly, my framework solely pertain to unilateral lure operations.

alternatives. I also delve deeper into the debates regarding the permissibility of unilateral alternatives under domestic and international law. The chapter concludes with an explanation of how I arrived at the core hypothesis. I outline the evidence from previous studies supporting my claims that cybercrime faces unique challenges related to the facts of the case, applicable laws, and political considerations.

In Chapter 3, I further explain the research methodology, including the strengths and weaknesses of this research design. I lay out the other potential methodologies I could have deployed and why those approaches were disfavored. I then detail elements of the interviews and case studies, such as interviewee selection and recruitment, questioning strategy, case selection, research ethics considerations, and data analysis. I close the chapter with a discussion of potential biases in the data and alternative hypotheses and how I sought to address those concerns.

In Chapter 4, I report my findings on the use of extradition and its alternatives in cybercrime prosecutions. The interviews suggest that unilateral alternatives, in the form of lure operations, are indeed applied more frequently in cybercrime cases as compared to other transnational crimes. However, I find this is not due to legal barriers. Dual criminality requirements, the political offense exception, and jurisdictional conflicts have not created a need for unilateralism. Rather, the need stems from challenges related to the facts of the case, namely the attribution challenge and remote nature of cybercrime, as well as political complications, such as a lack of political will and state sponsorship.

In Chapter 5, I seek to determine whether cybercrime may evolve in the same manner as other types of transnational crime. Specifically, I compare cybercrime to terrorism, drug trafficking, fraud and foreign corruption, and export control and sanctions violations. I find that cybercrime is not likely to evolve toward cooperation as in terrorism and drug trafficking prosecutions due to the entrenched political obstacles. Nor can it rely

on the perpetrator travelling as part of the conspiracy as occurs in drug trafficking, fraud and foreign corruption, and export control and sanctions cases. The remote nature of cybercrime means that offenders often have no business reason to travel. Plus, cybercrime prosecutions will continue to face the attribution challenge.

The findings of Chapters 4 and 5 reveal that the need for unilateralism appears here to stay. So, in Chapter 6, I set out a framework for when the use of unilateral lure operations may be advisable in cybercrime cases. This chapter explores how the existing legal justifications that have been advanced for the use of unilateralism in war crimes, terrorism, and drug trafficking cases may apply to cybercrime. I ultimately conclude that lure operations may be most prudent when 1) there are no viable and less intrusive alternatives; 2) there is a significant and imminent threat, 3) the crime is suspected to be motivated by private gain for the accused; 4) law enforcement does not engage in entrapment or coercion; and 5) the accused is guaranteed a fair trial with full due process protections.

In Chapter 7, I provide a brief recap of the key findings of this dissertation, explore their generalizability, outline their implications for international law and policy, and propose several directions for future research.

2. THEORIZING THE USE AND LEGAL IMPLICATIONS OF ALTERNATIVES TO EXTRADITION

Wanted! Stop in the name of the law! Securing custody over perpetrators of crime is an age-old problem that has beleaguered law enforcement. As wily criminals crossed borders to escape justice, law enforcement needed to develop mechanisms to lay their hands on these offenders. In response, victim countries negotiated extradition agreements with each other to facilitate rendering fugitives.

Although the extradition regime has persisted, it suffers from political and procedural challenges that undermine its effectiveness. Countries may simply refuse to sign extradition treaties or can even nullify existing agreements. Plus, the charged conduct must be illegal under both countries' laws, and the pursuing country must oftentimes satisfy onerous evidentiary requirements.

To address these concerns and the rise of transnational crime, countries have developed a system of transnational criminal law (TCL). The goal: to harmonize their criminal legislation and facilitate mutual legal assistance and extradition. However, these international conventions struggle with getting signatories to comply with their provisions and satisfactorily update their domestic statutes. As a result, victim countries have turned to alternatives to extradition to overcome these challenges and obtain custody over international fugitives. Some of these alternatives involve the host country's informal cooperation while others cut the host country completely out of the equation.

The use of alternatives to extradition has generated significant debate as to their lawfulness. Based United States court precedent, it generally does not matter how the defendant arrived at the courtroom. Law enforcement's conduct in securing custody simply must not shock the conscience. However, from an international law perspective, certain scholars contend that unilateral alternatives violate the sovereignty of the host

country and/or rights of the accused. Other scholars dispute these positions and point to various justifications under international law for the use of such methods to combat certain transnational crimes. As this debate continues, there have been no empirical studies to determine the factors that influence the application of alternatives to extradition.

This dissertation seeks to fill that void by examining why states apply unilateral alternatives. My goal is to determine whether any improvements in international law could facilitate cooperation and mitigate the reasons for their use. However, it may be that such challenges do not stem from legal issues alone and the need for unilateralism will remain. In that case, I will use these findings to develop an international framework that outlines baseline standards as to when the use of such alternatives may be prudent.

Additionally, there have been no studies investigating how states apply alternatives to extradition for a burgeoning area of transnational crime: cybercrime. That is a second void this dissertation aims to address. This will enable me to determine how the existing justifications for unilateralism can apply to this new form of criminality. Indeed, I argue that cybercrime poses distinct complications related to the facts of the case, applicable law, and political considerations, which increase the need for unilateralism. I predict, in turn, that pursuing countries are more likely to apply unilateral alternatives to extradition versus quasi-extradition and extradition in prosecutions of cybercrime as compared to other transnational crimes.

This chapter adopts the following structure. Section 2.1 discusses the challenges to the extradition regime. Section 2.2 examines the emergence of TCL and its limitations. Section 2.3 seeks to define alternatives to extradition and develop a taxonomy for categorizing these methods. Section 2.4 offers concrete examples of how alternatives to extradition have been applied in practice. Section 2.5 explores the legality of alternatives to extradition according to both US domestic law and international law. Section 2.6 applies

the existing literature to cybercrime to hypothesize how, if at all, the use of alternatives to extradition may differ as compared to other transnational crimes.

2.1 Extradition

Extradition's goal is to bring to justice criminals across borders. Yet, this tool has produced mixed results due to political and procedural barriers. In this section, I provide a brief overview of extradition and outline these key hurdles. Specifically, countries face no obligation to enter into extradition agreements. Even when such treaties exist, extradition can be stymied by dual criminality requirements, the political offense exception, evidentiary standards, and prohibitions on a country handing over its nationals.

According to McDermott, extradition refers to the formal process whereby state A renders an individual who has been accused or convicted of a crime in state B to state B so that the individual may be tried in state B's courts or face the punishment already determined there.[1] McDermott elaborates that countries enter such agreements out of self-interest. Cooperation with a pursuing country may result in future reciprocity if the extraditing country one day desires the return of a fugitive in the pursuing country.[2] Nevertheless, extradition has oftentimes failed to meet its promise.

The first challenge: there is no binding legal or moral obligation on countries to extradite unless they are party to a specific treaty. Therefore, they can choose whether to enter into extradition agreements with a given foreign nation based on the political preferences of their citizens or strategic interests. For instance, rival or enemy states may elect not to create a new treaty or to nullify an existing extradition agreement they share due to geopolitical tensions. Despite the overall growth of extradition agreements over the

[1] McDermott, "The Structure of International Cooperation in the Transfer of Suspects. Extradite or Abduct?," 255.
[2] McDermott, 272.

centuries, these political factors cause it to remain a patchwork quilt. Criminals can then exploit the gaping holes to seek safe haven.[3]

Likewise, extradition is impeded by various procedural protections. Specifically, dual criminality provisions require that the conduct be criminalized in both the pursuing and extraditing countries for extradition to proceed. Traditionally, this mandated that the charged crimes exactly match between both jurisdictions. However, states have increasingly relaxed this requirement to allow extradition merely when the substantive conduct is illegal in both locations.[4] Even still, these provisions prove troublesome. This is especially true as new conduct is criminalized in the pursuing country but no equivalent law is passed in the host country. Additionally, Nadelmann highlights that many foreign courts can be confused by certain US federal laws. One example is the use of wire fraud to prosecute schemes conducted using the phone or internet. These foreign courts may then deny extradition on the belief that there was no equivalent crime in their country.[5]

Another procedural hurdle is the political offense exception. Many extradition treaties prohibit rendering individuals for conduct that is directly or indirectly of a political character. It is important to note that this exclusion only refers to the nature of the offense, not any political motivations for the arrest. For example, a pursuing country would not be barred from seeking the extradition of a political dissident for say a car theft even if the prosecution was politically motivated. They could, however, be barred from seeking the extradition of that individual for his or her dissident behavior.

This exception is typically generic and open to interpretation by the courts. Nevertheless, there are three classes of political offense. First is pure, which refers to

[3] Prost, "No Hiding Place: How Justice Need Not Be Blinded by Borders," 126–27.
[4] Joutsen, "International Instruments on Cooperation in Responding to Transnational Crime"; Prost, "No Hiding Place: How Justice Need Not Be Blinded by Borders," 135–36; McDermott, "The Structure of International Cooperation in the Transfer of Suspects. Extradite or Abduct?," 288–89.
[5] Nadelmann, "The Evolution of United States Involvement in the International Rendition of Fugitive Criminals," 831.

prototypical political conduct like treason, sedition, subversion, espionage, and conspiracy to overthrow the government. These offenses are directed at the state and do not generally entail violence. Second is relative, which is "driven by a political agenda or occurring within a political context" and involves a common crime that affects private interests.[6] Third is indirect, which is a common crime connected with or in support of a political offense.

Countries usually follow one of three tests in determining whether a political offense has occurred. Under the political incidence test, courts look at whether the conduct was perpetrated by a member of a group involved in a political conflict to challenge their government. They also consider whether the conduct was in pursuit of that goal. Under the injured rights test, political offenses are those that "directly harm the rights of a State's political organization," irrespective of the motive.[7] Under the political predominance test, the courts examine the extent to which the act was politically motivated and the proportional weight of the political versus common crime components of the offense.

Extradition may also be hindered due to the procedural difficulty of meeting evidentiary requirements. This can be particularly challenging when extradition is requested between countries of differing legal traditions.[8] For instance, many common law countries mandate that the pursuing country submit the underlying evidence as well as a warrant. This evidence often must be presented in the format used in the host country, which may be foreign to the pursuing prosecutors. Furthermore, to avoid concerns over hearsay, each witness may be asked to provide a statement that is solely composed of their personal knowledge. These requirements may force prosecutors to develop an entirely new

[6] Sadoff, *Bringing International Fugitives to Justice*, 203.
[7] Sadoff, 206.
[8] McDermott, "The Structure of International Cooperation in the Transfer of Suspects. Extradite or Abduct?," 289; Prost, "No Hiding Place: How Justice Need Not Be Blinded by Borders," 137.

package of evidence. As prosecutors struggle to "meet an unknown standard, in a completely foreign format, it can prove to be an insurmountable hurdle to extradition."[9]

Some new or renegotiated extradition agreements have attempted to address these evidentiary issues. These treaties have eliminated the requirements that prosecutors follow the host country's rules of evidence and submit first person statements from witnesses. However, very few states have adopted these improvements.[10]

Equally problematic, the constitutions or domestic statutes of many states, namely those of the civil law tradition, prohibit the extradition of their nationals.[11] Theoretically, if two countries share an extradition treaty, this issue should be overcome by the principle of *aut dedere aut judicare*. In other words, the host country should either extradite or domestically prosecute. Nevertheless, Nadelmann and Prost both observe that host countries often lose interest in pursuing these cases or assign them lower priority. It can simply be too challenging to obtain evidence and secure the participation of victims and witnesses abroad.[12]

Evidently, despite extradition's objective of combatting transnational crime, this tool has frequently fallen short. It has been forestalled by political challenges as well as the procedural barriers of dual criminality, the political offense exception, evidentiary requirements, and non-extradition of nationals. While these impediments were intended to protect the rights of the accused, they have in many instances fostered impunity.

---

[9] Prost, "No Hiding Place: How Justice Need Not Be Blinded by Borders," 137.
[10] Prost, 138.
[11] Joutsen, "International Instruments on Cooperation in Responding to Transnational Crime"; McDermott, "The Structure of International Cooperation in the Transfer of Suspects. Extradite or Abduct?," 290; Prost, "No Hiding Place: How Justice Need Not Be Blinded by Borders," 140.
[12] Nadelmann, "The Evolution of United States Involvement in the International Rendition of Fugitive Criminals," 856; Prost, "No Hiding Place: How Justice Need Not Be Blinded by Borders," 140.

2.2 Transnational Criminal Law

In response to the weaknesses of extradition, states have turned to the passage of TCL to combat specific forms of transnational crime. I now walk through a brief overview of TCL and its key limitations, which are similar to those faced by the extradition regime. Namely, countries are not required to join TCL conventions and are given substantial liberty in how they implement their provisions. As a result, the effectiveness of TCL in helping bring transnational criminals to justice can be significantly curtailed.

These international suppression conventions oblige signatories to criminalize certain conduct in their domestic laws. The objective is to achieve greater harmonization of criminal laws between states. They also mandate that parties cooperate with transnational investigations by establishing extradition and mutual legal assistance mechanisms. While these conventions require that states outlaw certain behaviors, the power remains with the states to investigate and prosecute the offenses under their domestic criminal justice systems. Therefore, the signatories retain their sovereignty. Theoretically, these conventions would eliminate potential problems with dual criminality provisions by ensuring that the conduct is criminalized in all participating countries. They would also ideally widen the network of states bound to cooperate in such transnational criminal matters. However, TCL has faced its own political and procedural shortcomings that have prevented it from attaining its full potential.

Primarily, there is no international obligation for states to combat the crimes covered by TCL. So, states that do not wish to cooperate can simply elect not to ratify the suppression convention. They then have no responsibility to deal with the crime in their territory. This, in turn, can create a safe haven for perpetrators. Furthermore, many states do not enact the requisite domestic legislation. They may lose political motivation after

ratifying the agreement. Or they may realize that they simply do not have the resources. Regardless of the cause, this lack of follow through undermines the purpose of TCL.[13]

Even when states pass new domestic laws, TCL faces significant implementation issues that limit its success. For instance, TCL conventions are frequently drafted in a broad and ambiguous manner. On the one hand, this provides states with flexibility and garners greater support.[14] On the other hand, it means that states may adopt different definitions to fit the conventions to their culture and legal traditions or resolve domestic political compromises.[15] In the worst-case scenario, these definitions may vary so greatly between countries that courts may determine they do not refer to the same conduct. As a result, extradition requests may still fail to satisfy dual criminality requirements.

Moreover, many TCL conventions allow states to apply reservations. They can exempt themselves from specific sections, which can severely limit the convention's effectiveness.[16] Finally, TCL typically lacks monitoring and enforcement mechanisms to assess and ensure state compliance.[17] As a collective result of these shortcomings, Dandurand and Chen assert that "by most accounts and in most parts of the world, this international cooperation regime remains very weak, fragmented and capricious."[18]

2.3 Defining and Categorizing Alternatives to Extradition

Due to the inadequacies of extradition and TCL, states may be forced to either abandon the case or pursue an alternative to extradition.[19] In this section, I seek to define

[13] Dandurand and Chin, "Implementation of Transnational Criminal Law: Issues and Challenges," 440–41.
[14] Boister, "Responding to Transnational Crime: The Distinguishing Features of Transnational Criminal Law," 38.
[15] Dandurand and Chin, "Implementation of Transnational Criminal Law: Issues and Challenges," 441.
[16] Hui, Kim, and Wang, "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks."
[17] Dandurand and Chin, "Implementation of Transnational Criminal Law: Issues and Challenges," 442–43; Boister, "Transnational Criminal Law?"; Rose, "Treaty Monitoring and Compliance in the Field of Transnational Criminal Law."
[18] Dandurand and Chin, "Implementation of Transnational Criminal Law: Issues and Challenges," 439.
[19] McDermott, "The Structure of International Cooperation in the Transfer of Suspects. Extradite or Abduct?," 256.

and provide a brief history of such alternative approaches. I then review and assess the various taxonomies that international law scholars have developed to categorize alternatives to extradition. I conclude this section with my own taxonomy, which is based on the relationship between the pursuing and host countries. I divide such alternatives into two categories: quasi-extradition and unilateral alternatives.

This analysis will rely upon Sadoff's definition of alternatives to extradition. He describes these as "all measures, methods, and mechanisms, whether ultimately regarded as lawful or unlawful, that: (i) fall outside the extradition regime; (ii) aim to bring a fugitive to justice fully or partially, directly or indirectly; and (iii) do not entail a fugitive's delivery as a function of sheer fortuity."[20] Therefore, even though it does not involve extradition from the host country, waiting for the perpetrator to travel on his own to the pursuing country or a cooperative third country would not be an alternative to extradition. Securing custody in that manner would instead be a "function of sheer fortuity."

The US's use of alternatives to extradition can be traced to the 1866 rendition[21] of John Surratt, a conspirator in the Lincoln assassination, from Alexandria, Egypt. However, prior to the 1970s, such mechanisms were predominantly employed by law enforcement officials working near the border.[22] This changed with the heightened focus on international drug trafficking. The US Drug Enforcement Agency began implementing alternatives as a matter of "conventional wisdom." This practice soon spread to the Federal Bureau of Investigation and US Marshals Service.[23]

---

[20] Sadoff, *Bringing International Fugitives to Justice*, 605.
[21] In recent years, the term rendition has adopted a new meaning in the context of the War on Terror whereby terrorists were kidnapped and then brought to countries where they could be subject to enhanced interrogation. However, the term rendition in the context of this dissertation does not refer to this form of "extraordinary rendition" but rather its traditional meaning of surrendering a fugitive to another country.
[22] Nadelmann, "The Evolution of United States Involvement in the International Rendition of Fugitive Criminals," 860.
[23] Nadelmann, "The Evolution of United States Involvement in the International Rendition of Fugitive Criminals."

In the 21st Century, the application of alternatives has continued to grow as they have been applied to additional crimes such as terrorism. In fact, a 2001 US government report indicated that 600 criminals were extradited to the US that year. However, another 200, or 25%, arrived via other mechanisms.[24] These practices are not limited to the US either. Rather, they have been used worldwide to combat the rise of transnational crime.

In response to this growing trend, scholars have developed various taxonomies of the alternatives that states employ. Sadoff first divides the alternatives based on whether the outcome is functionally equivalent to extradition. Specifically, he creates two umbrella categories of fall-back alternatives and full-scale alternatives. Fall-back alternatives refer to "those partial or redirected means of bringing a fugitive to justice other than by extradition."[25] This comprises law enforcement actions such as arranging for a sealed indictment, creating an international wanted poster, or offering a reward for information. However, these methods cannot, on their own, bring fugitives to justice. In fact, they may have no impact whatsoever. It is also problematic to consider these mechanisms as alternatives to extradition since they may ultimately be used in conjunction with formal extradition from the host country.

In contrast, full-scale alternatives denote "those non-extradition-related means of bringing a fugitive to justice that functionally approximate the end result of extradition; namely, securing the physical custody of a fugitive and bringing him within a pursuing State's judicial system to be prosecuted or punished."[26] This dissertation solely focuses on full-scale alternatives since these mechanisms can, on their own, accomplish the central goal of bringing the fugitive to justice. To avoid introducing any possible biases in the data, this analysis considers both successful and attempted full-scale alternatives.

[24] Bassiouni, *International Extradition: United States Law and Practice*, 214.
[25] Sadoff, *Bringing International Fugitives to Justice*, 347.
[26] Sadoff, 391.

The remaining typologies simply focus on categorizing the full-scale alternatives. For instance, McDermott groups kidnapping, luring, and disguised extradition (i.e., deporting the criminal instead of using formal extradition processes) under the category of extraterritorial abduction.[27] However, this taxonomy faces issues since it groups three approaches that imply different relations between the pursuing and host countries. Although Poort recognizes the distinctions between these alternatives, his typology remains problematic. He divides the alternatives into the four categories of recuperation of the criminal in violation of international law, abduction of the criminal from state A by state B with or without state A's knowledge, abuse of immigration procedures, and unlawful arrest by state A before formally extraditing the criminal.[28] Nevertheless, Poort fails to clarify what is meant by "recuperation of the criminal in violation of international law" and why abduction is not just a subset of that category. He also overlooks the role of luring and does not explain how the fourth category is an alternative if the host country still engages in formal extradition proceedings.

Feinrider divides the alternatives even further into the seven categories of unilateral abduction by the pursuing country, abduction by the pursuing country with the aid of the host country, employment of the host country's agents by the pursuing country to abduct the fugitive, abduction by third parties, informal rendition by the host country, and expulsion through immigration procedures.[29] Yet, this grouping again ignores the role of luring. It also excessively partitions alternatives despite the relationship between the pursuing and host countries remaining the same. For example, it separates abduction with the aid of the host country, informal rendition by the host country, and expulsion through immigration procedures even though the host country cooperates in all three categories.

[27] McDermott, "The Structure of International Cooperation in the Transfer of Suspects. Extradite or Abduct?," 256.
[28] Poort, "Male Captus, Bene Judicatus: Disguised Extradition and Other Practices," 66.
[29] Feinrider, "Extraterritorial Abductions: A Newly Developing International Standard," 27–28.

Abramovsky and Eagle, Evans, Bassiouni, and Sadoff provide the most helpful taxonomies of full-scale alternatives. These scholars divide them based on the degree of cooperation between the pursuing and host countries. For instance, Abramovsky and Eagle group the alternatives into unilateral abductions by the pursuing country and irregular renditions. In the latter, the host country either cooperates with or permits the removal of the fugitive from their territory.[30] Evans adopts a similar division between unilateral abductions and arrests in which the host country cooperates. Nevertheless, she uses the term irregular rendition to refer to kidnapping and focuses more on instances when the host country uses immigration laws to render the fugitive.[31] Bassiouni espouses a hybrid of these classification approaches with three categories: abduction, informal rendition of the fugitive by the host country to the pursuing country, and the use of immigration procedures.[32] Sadoff adopts a nearly identical typology but broadens unilateral action to include other alternative approaches, such as luring, and is thus the most comprehensive.

Based on the above literature, I adopt the following taxonomy of full-scale alternatives to extradition. I divide them according to whether there is cooperation between the pursuing and host countries.

1. Quasi-extradition whereby the host country cooperates in rendering the fugitive outside of the formal extradition process, such as by using immigration laws to deport the fugitive or informally handing over the fugitive; and
2. Unilateral alternatives to extradition whereby the pursuing country seeks to secure custody of the fugitive outside of the formal extradition process and without the involvement of the host country or the host country's agents acting in their official capacity, such as via luring, kidnapping, or interception.

[30] Abramovsky and Eagle, "U.S. Policy in Apprehending Alleged Offenders Abroad," 52.
[31] Evans, "Acquisition of Custody over the International Fugitive Offender - Alternatives to Extradition: A Survey of United States Practice," 82–89.
[32] Bassiouni, "Unlawful Seizures and Irregular Rendition Devices as Alternatives to Extradition."

2.4 Examples of Alternatives to Extradition

To elaborate upon these categories, this section provides specific examples of quasi-extradition and unilateral alternatives to extradition.

Under quasi-extradition, the host country may utilize immigration laws to either exclude the fugitive from entering the country at the border or deport him at the pursuing country's request. Deportation can be formal through official channels, informal through casual arrangements, or voluntary.[33] However, removal procedures typically result in the individual being returned to his home country. So, states have developed a clever workaround when the pursuing country is not the fugitive's home. The fugitive is deported to his home country via a layover in the pursuing country. He is then promptly arrested upon arrival in the pursuing country. In other cases where there is no legal basis to deport the fugitive to the pursuing country, the host country may remove the fugitive to a third country that has legal standing to receive the individual. That third country may subsequently render him to the pursuing country.[34] Host countries may rely upon immigration laws to render the fugitive since this approach can overcome procedural barriers to extradition, such as the lack of a treaty, dual criminality requirements, the political offense exception, and evidentiary burdens.[35]

Quasi-extradition also incorporates any instance whereby agents of the host country, acting in their official capacity with their approval of their government, assist in rendering the fugitive to the pursuing country outside of any legal procedures. They may aid in the abduction of the fugitive. Or, they may arrest the perpetrator and then deliver him to the pursuing country without extradition proceedings. Furthermore, quasi-extradition may take the form of host country acquiescence. In this scenario, the pursuing

[33] Sadoff, *Bringing International Fugitives to Justice*, 397–400.
[34] Sadoff, 408.
[35] Bassiouni, *International Extradition: United States Law and Practice*.

country may abduct or arrest the fugitive in the host state territory with the host country's approval.[36] Informal handovers and acquiescence similarly address some of the political and procedural challenges of extradition. For instance, the host country may have a law enforcement interest in the fugitive's removal. Yet, a formal extradition or deportation may generate public backlash, creating domestic political costs for leaders in the host country. Thus, informal cooperation enables them to covertly render the fugitive.[37]

Although unilateral alternatives may involve third states, they cannot include agents of the host country acting in their official capacities. Unilateral alternatives typically take the form of seizure and delivery operations (SDOs), lure and capture operations (LCOs), and interceptions. In SDOs, agents of the pursuing country clandestinely kidnap the fugitive in the host country and transport him to the pursuing country to face justice.

In LCOs, the criminal is convinced to travel to the pursuing country or a third country. The ruse may be for a commercial or professional activity such as a job interview. It may be for a social, personal, or recreational activity such as a vacation. Or, it may be for a law enforcement-related activity such as the opportunity to "clear his name." In certain cases, the criminal may know he is wanted in the pursuing country. So, he may be lured to a third country that will then extradite to the pursuing country or cooperate through a quasi-extradition.

Finally, in interception operations, the pursuing country employs force or the threat of force while the fugitive is traveling. Their objective is to divert his mode of transportation to land in either the pursuing country or a third country from which he can be rendered.[38] All three sub-categories of unilateral alternatives resolve each of the

[36] Sadoff, *Bringing International Fugitives to Justice*, 454–67.
[37] Sadoff, 456–57.
[38] Sadoff, 481–98.

political and procedural barriers to extradition. They circumvent all formal mechanisms and cut out the involvement of the host country, which may oppose rendition.

2.5 Debating the Legality of Unilateral Alternatives to Extradition

The academic literature on the use of alternatives to extradition, specifically unilateral alternatives, has predominantly focused on considering whether these mechanisms violate US domestic law and international law. I now review and synthesize that literature. On the one hand, there is a clear consensus that unilateral alternatives are permissible under US domestic law as long as they do not shock the conscience. On the other hand, there is significant disagreement as to their status under international law. Some scholars claim they violate the sovereignty of host country and human rights of the accused. Others dispute this position and outline specific conditions under which the use of unilateral tools may be justified for certain transnational crimes. I end by identifying several gaps in the literature, which this dissertation seeks to fill.

Since the late 1800s, US courts have consistently applied the Roman law maxim of *male captus, bene judicatus* to uphold the legality of unilateral alternatives. This principle states that a defendant whose custody is irregularly obtained can still be legally tried. It was first applied to unilateral alternatives in the case of *Ker v. Illinois*. Ker was indicted in Illinois for embezzlement and larceny but was residing in Peru. US law enforcement sent an extradition request to the host country. But, Peru was occupied by Chilean forces at the time, so the request could not be executed. Thus, the investigating officer resorted to kidnapping the defendant and transporting him back to the US.

The US Supreme Court ruled that extradition treaties do not prevent a party from using other means to obtain custody over a fugitive.[39] Additionally, the Court held that this abduction did not violate the defendant's rights since "'due process of law' . . . is complied

[39] Abramovsky and Eagle, "U.S. Policy in Apprehending Alleged Offenders Abroad," 54.

with when the party is regularly indicted by the proper grand jury in the state court, has a trial according to the forms and modes prescribed for such trials, and when, in that trial and proceedings, he is deprived of no rights to which he is lawfully entitled."[40]

This decision was reaffirmed in *Frisbie v. Collins*. In that case, the defendant was abducted and brought across state lines to be prosecuted. Once again, the US Supreme Court held that due process requirements are satisfied if the defendant is informed of the charges and receives a fair trial.[41]

In the 1980s, US courts deviated from these longstanding precedents. In *United States v. Toscanino*, an Italian citizen charged with narcotics offenses alleged that the US government had conspired with the police of Montevideo and a group of Brazilian citizens to kidnap him from Uruguay. He further asserted that during his captivity in South America, he had been beaten, drugged, and tortured. Therefore, the US Court of Appeals for the Second Circuit declined to apply the *Ker-Frisbie* doctrine. The court ruled the defendant's kidnapping violated his due process rights.[42]

While this case appeared to set a new precedent barring forcible abduction, the Second Circuit limited its application several months later in *United States ex rel. Lujan v. Gengler*. The court held that forcible abduction is permissible as long as it does not involve "conduct of the most shocking and outrageous character" like torture and brutality. Such conduct would rise to the level of violating due process.[43] Since then, US courts have consistently upheld the use of unilateral alternatives, including kidnappings, which has demonstrated their domestic legality.

However, the lawfulness of these mechanisms under international law remains the subject of continuing debate between legal academics. For example, Sadoff explains that

[40] *Ker v. Illinois*, 119 U.S. 436, 440 (1886).
[41] *Frisbie v. Collins*, 342 U.S. 519, 522 (1952).
[42] *United States v. Toscanino*, 500 F.2d 267, *rehearing denied,* 504 F.2d 1380 (2d Cir. 1974).
[43] *United States ex rel. Lujan v. Gengler*, 510 F.2d 62, 65 (2d Cir. 1975).

unilateral alternatives may violate the territorial sovereignty of the host country. States have an exclusive right to exercise law enforcement action over their territory. This has been clearly established in international law through the UN Charter, UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, and various General Assembly and Security Council Resolutions. Sadoff notes that this principle has now also assumed the status of customary international law as demonstrated by countless examples of state practice.[44] SDOs would clearly pose a threat to the host country's sovereignty since the pursuing country's law enforcement directly seize the fugitive from the host country's territory. LCOs may also breach the host country's sovereignty since the trick is carried out, at least partly, in the host country's territory.[45]

Nevertheless, other legal scholars contend that unilateral alternatives do not necessarily violate the host country's sovereignty. Gurulé maintains that unilateral alternatives, including kidnappings, are not directed against the political independence or territorial integrity of the host country and hence do not violate their sovereignty.[46] With respect to LCOs specifically, Sadoff elaborates that these tools are "not directed at the host State but rather at an individual … [and] its reliance on sovereign territory to effect the deceit tends to be incidental at most."[47]

Additionally, SDOs and interception operations may violate international law as illicit uses of force. Specifically, Article 2(4) of the UN Charter directs states to avoid the use of force against the territorial integrity or political independence of another state. Article 19 of the Charter of the Organization of American States similarly prohibits states from interfering in the internal or external affairs of another state.

---

[44] Sadoff, *Bringing International Fugitives to Justice*, 510–16.
[45] Sadoff, 506.
[46] Gurulé, "Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad," 486.
[47] Sadoff, *Bringing International Fugitives to Justice*, 505.

However, Sadoff notes that unilateral alternatives may not be illicit uses of force since they do not target the territorial integrity of the host country. Indeed, the goal of such treaties prohibiting the use of force is to protect countries' economic and political independence, which is not threatened when merely a single person is captured. Sadoff declares, "A forceful limited seizure of a fugitive within another's territory, after all, is not force directed against the State itself as much as against private rights."[48] Moreover, he specifies that the use of force typically refers to armed force, which may not necessarily be employed in an SDO.[49]

Unilateral alternatives may also run afoul of international human rights law. Bassiouni explains that these methods may contravene the Universal Declaration of Human Rights, which states in Article 9 that "no one shall be subjected to arbitrary arrest, detention or exile."[50] He expounds the Declaration is legally binding as an interpretation of the UN Charter.[51] Likewise, Article 9(1) of the International Covenant on Civil and Political Rights (ICCPR) affirms, "Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law."[52] The European Convention for the Protection of Human and Fundamental Freedoms and Inter-American Convention on Human Rights similarly contain provisions that Bassiouni argues would outlaw unilateral alternatives. He further asserts that every fugitive has a general right to due process, which can be inferred from human rights law.[53]

[48] Sadoff, 522.
[49] Sadoff, 522–23.
[50] Bassiouni, "Unlawful Seizures and Irregular Rendition Devices as Alternatives to Extradition," 54.
[51] Bassiouni, 55.
[52] "International Covenant on Civil and Political Rights."
[53] Bassiouni, "Unlawful Seizures and Irregular Rendition Devices as Alternatives to Extradition," 56.

Feinrider, Abramovsky and Eagle, and Evans all raise similar concerns that unilateral alternatives violate the rights of the accused.[54] Evans elaborates that the formal extradition process ensures that various conditions are met before a defendant is handed over to the pursuing country. The extradition hearing also provides an opportunity for the accused to challenge his rendition. These safeguards are simply not present for a unilateral alternative.[55] Abramovsky and Eagle likewise note that unilateral alternatives "do not afford the individual whose apprehension is sought a hearing to determine whether prima facie evidence exists to justify his removal."[56] Furthermore, Sadoff highlights that SDOs in particular may infringe on the fugitive's due process rights if he is not permitted to notify family or consular officials of his arrest, not promptly informed of the charges against him, or not provided an opportunity to promptly challenge the legality of his arrest before a court.[57]

Despite these arguments, other legal scholars believe that unilateral alternatives do not infringe upon the rights of the accused. Findlay reflects that no international treaty or convention prohibits abductions as a violation of international human rights. He also takes issue with Bassiouni's claims related to the Universal Declaration and ICCPR. Primarily, he disputes that the Universal Declaration constitutes customary law and views it more as "an aspirational document without legally binding force."[58]

Moreover, Findlay clarifies that Article 9(1) of the ICCPR has been interpreted to only require that states have a lawful reason to arrest an individual and procedures for their detention and prosecution. Nothing in that provision would therefore preclude a unilateral

---

[54] Feinrider, "Extraterritorial Abductions: A Newly Developing International Standard"; Abramovsky and Eagle, "U.S. Policy in Apprehending Alleged Offenders Abroad," 92.
[55] Evans, "Acquisition of Custody over the International Fugitive Offender - Alternatives to Extradition: A Survey of United States Practice," 98–99.
[56] Abramovsky and Eagle, "U.S. Policy in Apprehending Alleged Offenders Abroad," 92.
[57] Sadoff, *Bringing International Fugitives to Justice*, 532–33.
[58] Findlay, "Abducting Terrorists Overseas for Trial in the United States: Issues of International and Domestic Law," 35.

alternative.[59] Indeed, Kallenbach contends that a unilateral alternative cannot be considered an arbitrary arrest since it is still based on an indictment or conviction. In other words, the indictment provides the grounds for the arrest, and the subsequent criminal trial satisfies the procedural requirements of Article 9(1).[60]

According to Findlay, other sections of the ICCPR similarly cannot be construed to outlaw unilateral alternatives. For example, Article 12 provides "the right of liberty of movement." Yet, that protection only applies within a territory. Article 13 ensures that individuals cannot be expelled from a country without the opportunity to challenge such expulsion. However, a unilateral alternative is not an expulsion since the host country's officials are not involved in the operation.[61]

Findlay also challenges Evans and Abramovsky and Eagle's claims regarding the due process protections of the extradition process. He argues, "Extradition arrangements exist primarily for the benefit of the states involved, so an individual's rights cannot be said to have been violated if abduction denies her recourse to the extradition process."[62]

In addition to these general defenses of unilateral alternatives, certain legal scholars have outlined conditions or circumstances under which the use of these tools may be permissible under international law for specific crimes. For example, Kovac and Scharf examine when unilateral methods may be justified to bring war criminals to justice.[63] Calica, Findlay, and Gurulé engage in a similar exercise with respect to terrorism

[59] Findlay, 36.
[60] Kallenbach, "Plomo O Plata: Irregular Rendition as a Means of Gaining Jurisdiction over Colombian Drug Kingpins," 212–13.
[61] Findlay, "Abducting Terrorists Overseas for Trial in the United States: Issues of International and Domestic Law," 37.
[62] Findlay, 35.
[63] Scharf, "Case Analysis: The Prosecutor v. Slavko Dokmanovic: Irregular Rendition and the ICTY"; Kovac, "Apprehension of War Crimes Indictees: Should the United Nations' Courts Outsource Private Actors to Catch Them."

prosecutions while Fletcher, Kallenbach, McAlister, and McCarthy consider this question for drug trafficking cases.[64]

Despite these debates, there have been limited attempts in the literature to examine the factors that influence a pursuing country's decision to apply unilateral alternatives. For example, Abramovsky and Eagle, Sadoff, and McDermott simply assert that states resort to alternatives when extradition is unavailable. The case must also be sufficiently serious or a high priority. Evans offers a slightly more detailed explanation that a pursuing country may apply these alternatives when extradition is not available, would be unduly costly, or presents an unattainable evidentiary burden.[65] Of these scholars, only Sadoff explains how states decide between alternatives to extradition, arguing that unilateral action is a last resort.[66]

Therefore, I seek to fill this void by empirically determining the explanatory factors in a pursuing country's decision to implement unilateral alternatives. This will enable me to help identify what, if any, improvements in international law can be made to mitigate the use of unilateral methods. If such improvements are not possible, determining the explanatory factors is still useful. It will enable me to formulate an international framework that outlines the limited circumstances when cooperation and international law cannot overcome the core challenges of bringing perpetrators to justice and unilateralism

[64] Calica, "Self-Help Is the Best Kind: The Efficient Breach Justification for Forcible Abduction of Terrorists"; Findlay, "Abducting Terrorists Overseas for Trial in the United States: Issues of International and Domestic Law"; Gurulé, "Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad"; Fletcher, "Pirates and Smugglers: An Analysis of the Use of Abductions to Bring Drug Traffickers to Trial"; Kallenbach, "Plomo O Plata: Irregular Rendition as a Means of Gaining Jurisdiction over Colombian Drug Kingpins"; McAlister, "The Hydraulic Pressure of Vengeance: United States v. Alvarez-Machain and the Case for a Justifiable Abduction"; McCarthy, "United States v. Verdugo-Urquidez: Extending the Ker-Frisbie Doctrine to Meet the Modern Challenges to Posed by the International Drug Trade."

[65] Evans, "Acquisition of Custody over the International Fugitive Offender - Alternatives to Extradition: A Survey of United States Practice," 93–96.

[66] Sadoff, *Bringing International Fugitives to Justice*, 483.

may thus be prudent. Such a framework would assist pursuing countries in navigating the ongoing legal ambiguity they currently face in deploying unilateral alternatives.

2.6 Hypothesizing the Use of Alternatives to Extradition in Cybercrime Cases

As outlined above, the existing literature on alternatives to extradition has principally focused on the use of these mechanisms to combat war crimes, terrorism, and drug trafficking. There has been no investigation, to my knowledge, of their application to one of the fastest growing areas of transnational crime: cybercrime. Consequently, this dissertation seeks to fill that second void in the literature. This will enable me to determine the extent to which the existing justifications for unilateralism can apply to cybercrime.

According to Sadoff, states rely upon unilateral alternatives as a last resort. Extradition or removal via immigration procedures are not options or likely to fail. The host country is not expected to prosecute the offense domestically. And cooperation is not possible. These barriers may stem from legal impediments, strained political relations with the host country, or concerns over corruption within the host country's law enforcement. Likewise, the pursuing country may not believe that it can wait for extradition or quasi-extradition. The delay may simply offer the fugitive an opportunity to abuse the process or seek special treatment.[67]

Sadoff explains that the rare usage of unilateral alternatives stems from the questionable lawfulness of such a drastic step and its political implications. He specifies that unilateral action may damage the pursuing country's diplomatic relationship with the host country. It may jeopardize future cooperation on other international issues. And it may undermine respect for international law and the broader system of extradition.[68]

[67] Sadoff, 483–84.
[68] Sadoff, 588–90.

The focus of this dissertation on cross-border cybercrime now raises the question, is it a unique form of transnational crime? If so, is the likelihood that unilateral alternatives will be deployed any different for cybercrime?

In the first subsection, I contemplate the similarities between cybercrime and other cross-border offenses and how this may affect the methods used to secure custody. I ultimately argue that cybercrime faces unique complications related to the facts of the case, applicable laws, and political considerations. I explore each of these sets of obstacles in the three subsections that follow. Based on these challenges, I conclude with the prediction that there will be a greater usage of unilateral alternatives versus extradition and quasi-extradition in cybercrime cases as compared to other transnational crimes.

2.6.1 Cybercrime: Old Wine in New Bottles?

At first glance, cybercrime appears relatively similar to its real-world predecessors. Brenner notes that cybercrime "simply represents the migration of real-world crime into cyberspace." [69] Perpetrators merely use novel technologies to commit long-standing offenses. This new dimension does not change the underlying criminal conduct or harm inflicted on the victim. In fact, Brenner and Hayes et al. both note that many seemingly new offenses can be analogized to real-world crimes. Hacking is essentially trespass, cracking is a form of burglary, and software piracy is theft of intellectual property.[70]

Equally important, since extradition treaties are not specific to offenses, the same agreements that govern drug trafficking, organized crime, or terrorism would apply to cybercrime. Therefore, the same political and procedural barriers to extradition, such as dual criminality, evidentiary requirements, and non-extradition of nationals, would also

[69] Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*.
[70] Brenner, "Is There Such a Thing as 'Virtual Crime'?"; Hayes et al., "The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-Up?," 20.

afflict cybercrime cases. These shared challenges should accordingly result in a similar need for unilateralism, regardless of the crime.

Furthermore, the traditional basis for jurisdiction, territoriality, equally applies to cybercrime as real-world crime. This jurisdictional principle holds that states have the right to prosecute illicit behavior that occurs within their territorial boundaries.[71] Upon initial examination, transnational cybercrime would appear to pose complications for this jurisdictional basis. After all, it is often unclear whether the offense occurred where the cybercrime was initiated or where the impact ensued.

However, Clough and Sadoff observe that throughout history, states have largely accepted the principle of "objective territoriality." This jurisdictional basis permits them to prosecute crimes that result in some harm within their borders, even if the perpetrator never entered their territory.[72] Therefore, under objective territoriality, states would indeed have the right to prosecute transnational cybercrime. This would suggest that these offenses do not require any special treatment.

2.6.2 Challenges Related to the Facts of the Case

Nevertheless, I contend there are factual distinctions in how cybercrime is perpetrated as compared to other forms of transnational crime. Primarily, Brenner notes that cybercrime is often committed virtually from thousands of miles away. The perpetrator does not need to ever be physically present at the scene of the crime.[73] This thereby increases the difficulty of bringing the perpetrator to justice. Unlike a drug trafficker or terrorist, a cybercriminal may never enter the victim state's jurisdiction where he can be arrested. As a result, the victim state must rely more heavily on formal extradition or its alternatives.

---

[71] Grabosky, "The Global Dimension of Cybercrime," 151.
[72] Clough, *Principles of Cybercrime*, 476; Sadoff, *Bringing International Fugitives to Justice*, 74–75.
[73] Brenner, "Distributed Security: A New Model of Law Enforcement."

When extradition or quasi-extradition fail, the victim state also faces a greater need to resort to unilateralism. They cannot simply wait for the perpetrator to travel to their jurisdiction. There is no business reason for the offender to do so. Thus, the victim country more frequently needs to take affirmative unilateral action to lay hands on the defendant.

Equally important, automation technologies permit cybercriminals to more easily target hundreds or thousands of victims at once.[74] In fact, Clough describes cybercrime as a "force multiplier. It enables crime to be perpetrated on a scale generally not possible offline.[75] Moreover, cybercriminals can commit their offenses with less physical effort than that required for real-world crimes.

Cybercrime may seem to have high barriers to entry. But, the internet and underground online marketplaces allow anyone to purchase easy-to-use hacking software. Amateurs can now even hire the services of an experienced cybercriminal on the dark web.[76] Due to this lack of physical constraints and the corresponding ease of committing cybercrime, perpetrators can not only target an astounding number of victims. They can also victimize individuals from multiple countries simultaneously.

Brenner notes that cybercrimes are more likely to consist of severable offenses. In other words, a cybercriminal hacking individual A in country X is often a distinct crime from that cybercriminal hacking individual B in country Y. This contrasts with, for example, bombing a plane containing citizens from countries A, B, and C. In the latter case, one crime is committed against citizens of three countries rather than three separate offenses.[77]

Since cybercrime is more likely to target victims from multiple countries via severable offenses, Brenner notes that it generates jurisdictional complexities. Specifically,

---

[74] Brenner, 10.
[75] Clough, *Principles of Cybercrime*, 6.
[76] Clough, 7.
[77] Brenner, "Cybercrime Jurisdiction," 199.

the global spread of cybercrime victims commonly results in "an *excess* of jurisdiction." Each victimized country wishes to prosecute the offender for the same conduct.[78] With real-world transnational crime, Brenner explains that a victimized country usually does not lose if it cannot prosecute the offender first. That criminal can still be brought to justice elsewhere for the same behavior. However, each cybercrime is more likely to be severable. So, Brenner claims that one state's prosecution of the cybercriminal for his offenses against its citizens does not satisfy the other victimized states' desire to prosecute.[79]

2.6.3 Legal Obstacles

Unfortunately, there is no clear mechanism under international law to resolve overlapping jurisdictional claims. This ambiguity is exacerbated in cases of cybercrime. Ordinarily, states weigh the "location of the offense and offender, the nationality of the offender and victims, the degree of harm that was caused, [and] the location of the evidence."[80] Nevertheless, Clough maintains that there is less of a correlation between these factors in cybercrime. Accordingly, it can become more difficult for states to reconcile multiple jurisdictional claims in cybercrime versus other transnational crimes. For example, in contrast to offline crime, the cybercriminal is often not in the same location as the victim.[81] Likewise, it is ambiguous if the state where the cybercrime was initiated or where the impact occurred deserves jurisdictional primacy.

As a result, I maintain that there is a lower probability that the host country will prioritize a given pursuing country's jurisdictional claims in a cybercrime case. This may stem from an overarching lack of interest on part of the host country. Or it can arise from disagreement over which factors are most important in determining where the cybercriminal should be prosecuted. Therefore, I predict that these jurisdictional conflicts

[78] Brenner, 196.
[79] Brenner, 199.
[80] Clough, *Principles of Cybercrime*, 485.
[81] Clough, 485.

increase the likelihood that pursuing countries will undertake unilateral action to preempt other pursuing countries and bring the fugitive to justice in their domestic courts.

Equally important, I propose that the distinct lack of legal harmonization on cybercrime precludes formal extradition. This thereby increases the probability that states will employ alternative approaches. Specifically, I posit that many countries have not enacted adequate domestic legislation as new online threats emerge. Cybercrime is not like drug trafficking, financial fraud, corruption, or other transnational crimes that have been around for years and thus already outlawed by criminal statutes in host countries.

A 2013 study by the UN Office on Drug and Crime (UNODC) discovered that less than half of the countries that responded considered their substantive and procedural laws adequate to combat cybercrime. These challenges were particularly pronounced in Africa, the Americas, Asia, and Oceania where only one third reported having sufficient legislation. Of these countries with inadequate laws, only half reported that legislative improvements were in the works. As a result, only one third of reporting countries stated that their laws were highly or very highly harmonized with the countries they consider critical for international cooperation on cybercrime.[82]

It is important to note that the failure of states to adopt cybercrime legislation is not merely a time-series effect. It is not merely due to the novelty of these offenses. Rather, Goodman and Brenner explain it is often due to a lack of interest, anticipated incompatibility of proposed cybercrime legislation with existing national laws, or disagreement with the underlying penal philosophy.[83] Likewise, certain countries have focused on only outlawing cybercrimes committed against domestic computers, erecting a further legal barrier for pursuing countries.[84]

[82] UN Office on Drugs and Crime, "Comprehensive Study on Cybercrime," xviii–xvix.
[83] Goodman and Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace," 216.
[84] Shull, "Global Cybercrime: The Interplay of Politics and Law," 12.

States have attempted to address these issues through the enactment of TCL. However, I contend that the sole international convention on this topic, the Council of Europe Convention on Cybercrime (Budapest Convention), has failed to adequately harmonize cybercrime laws and ensure international cooperation. The Convention has relied on vague definitions of the key offenses, leaving the interpretation up to its signatories.[85] As a result, UNODC found considerable differences between the domestic legislation enacted by the signatories. This means that illegal online conduct in one state may remain permissible in another. In turn, dual criminality may not be satisfied for an extradition request related to such conduct.

Moreover, the Budapest Convention does not include new cybercrimes that have emerged since the 1990s, such as data espionage and spamming.[86] These offenses could be addressed through drafting new protocols to the Convention, but this has not occurred. The failure to draft new protocols is again not merely an instance of regulatory lag. Instead, it reflects a broader difference of perspective between the treaty's signatories. For instance, developed countries tend to view spam as a civil or administrative concern while developing countries consider it a criminal matter.[87]

Additionally, the Budapest Convention has allowed signatories to condition their agreements on various declarations and reservations, which can further water down its effectiveness. The US alone registered twelve reservations to the Convention. Plus, this treaty provides states with broad opportunities to refuse cooperation. They can simply claim that assisting in an investigation would prejudice an essential interest like their national security or sovereignty. The potentially emasculating effects of these loopholes are exacerbated by the treaty's lack of any enforcement mechanism. There is no formal

[85] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 3.
[86] Boister, *An Introduction to Transnational Criminal Law*, 195.
[87] Clough, "A World of Difference: The Budapest Convention and the Challenges of Harmonisation," 703.

way to ensure that its signatories meet their obligations to update their laws and collaborate with investigations. As a result, Goldsmith argues that "signatories often flout or ignore the cooperation provisions."[88]

The effectiveness of the Budapest Convention is further limited by geography. It has not reached the point of becoming a truly universal cybercrime treaty. This failure is also not simply a time-series effect that is likely to disappear in the years to come. Part of the difficulty in achieving widespread adoption stem from the treaty's regional origins at the Council of Europe. According to Goldsmith, certain countries have refused to sign the treaty due to its "its definitions of crimes (for example, the criminalization of intellectual-property violations), its general Western focus, or its (weak) sovereignty-intrusive cooperation mechanisms."[89] These countries include China, Iran, North Korea, and Russia, all of which are concerns for cybercrime. Their refusal to join the Budapest Convention means that they face no obligation to enact adequate cybercrime legislation nor cooperate in international investigations. Thus, cybercrime laws may not be harmonized with these countries, and dual criminality requirements may not be satisfied.

This failure to widely adopt the Budapest Convention stands in stark contrast to the existing TCL related to other cross-border offenses. For example, the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances has 190 parties, which includes 185 out of the 193 UN member states. The UN Convention against Transnational Organized Crime has 189 parties, including 184 member states. The Convention for the Suppression of Unlawful Seizure of Aircraft has 186 parties. And the UN Convention against Corruption has 187 parties, including 181 member states.

[88] Goldsmith, "Cybersecurity Treaties: A Skeptical View," 4.
[89] Goldsmith, 4.

Due to the lack of sufficient legislation in host countries and failure of the Budapest Convention to bridge this gap, I expect that cybercrime is more likely than other transnational crimes to face dual criminality concerns. Given that this legal barrier blocks extradition, I predict that there will, in turn, be a need for greater reliance on alternatives to extradition for cybercrime as compared to other transnational crimes.

The political offense exception presents a further legal obstacle that may make extradition less likely to succeed for cybercrimes than other transnational crimes. As cybercriminals increasingly operate under the auspices or direction of state sponsors, they may claim that their conduct is simply a form of espionage. A similar defense could be raised for hacktivists. These individuals hack into and release sensitive private information from the networks of corporations, government entities, and individuals to bring about political or societal change. They could claim that their cybercrimes were driven by or in furtherance of a political agenda.

In these cases, the host country could be legally barred from granting extradition. It could also preclude waiting for the cybercriminal to travel to another country. Given the ubiquity of political offense exceptions in extradition treaties, such third countries could still be legally barred from granting extradition. Once again, the pursuing country may face a pressing need to turn to alternatives to extradition to render the fugitive directly to their territory and skirt political offense barriers.

This need is likely greater than that experienced for other transnational crimes. It would be difficult for an international fugitive to credibly claim that drug trafficking, financial fraud, or foreign corruption was in furtherance of a political agenda against the pursuing country. While certain Colombian narcotraffickers were involved in that country's internal armed conflict, their political actions were not directed against the

countries into which they were pumping drugs. So, the political offense exception would not likely block an extradition request from one of those victim countries.

One other area of transnational crime where the political offense exception could be a barrier is international terrorism. Indeed, it would be easy for a perpetrator to claim their crimes were to accomplish a political objective against the state or raise international awareness of a political issue.

However, given the significant threat to innocent lives from terrorist attacks, the international community has increasingly limited the applicability of the political offense exception to terrorism. As Sadoff notes, "… particularly with respect to terrorism, its reach has been markedly circumscribed in recent years in a number of crime suppression and extradition treaties, U.N. documents, and domestic extradition statutes."[90] In fact, the 1977 European Convention on the Suppression of Terrorism, 1998 International Convention on the Suppression of Terrorist Bombings, 1999 International Convention on the Suppression of the Financing of Terrorism, and the 2005 International Convention for the Suppression of Acts of Nuclear Terrorism do not include a political offense exception.[91]

2.6.4 Political Complications

In addition to these factual complications and legal barriers, cybercrime presents various political challenges, which I posit prevent relying on international cooperation. This thus encourages pursuing countries to resort to unilateral action. For instance, host countries are more likely to lack the political will to combat cybercrime as compared to other transnational crimes. The victim is simply harder to empathize with since they are often located far away from the host country. Host countries would rather focus their efforts on offenses that affect their citizens, especially when they have limited law

[90] Sadoff, *Bringing International Fugitives to Justice*, 209.
[91] Sadoff, 209.

enforcement capacity.[92] The distance between perpetrator and victim in cybercrime thereby diminishes the host country's interest in prosecuting domestically, extraditing, or cooperating through a quasi-extradition. Pursuing countries are then more frequently left with unilateral alternatives as their only option to bring the cybercriminal to justice.

For other types of transnational crimes such as drug trafficking, terrorism, financial fraud, or foreign corruption, there is a greater risk of the perpetrator generating local harms. These other offenses are not like cybercrime where the deleterious effects are typically confined abroad. Drug trafficking, for instance, frequently engenders corruption and violence in the host country. These domestic harms therefore increase the host country's incentives to address the threat internally or cooperate in cross-border prosecutions. This buy-in from host countries means that there is less of a need for unilateralism as compared to cybercrime. A similar logic applies to terrorism whereby there is a risk that such perpetrators may begin launching attacks domestically. Therefore, host countries have a pressing interest in cooperating to eliminate that threat.

Additionally, as Soma and Muther contend, states have not reached universal international consensus on combatting cybercrimes such as computer hacking, threats to national security, computer stalking, and electronic theft.[93] States differ in their views as to whether certain conduct online should be considered a criminal violation as well as the seriousness of cybercrimes.[94] Indeed, the lack of international consensus can be observed in the limited reach of the Budapest Convention, which has largely remained a regional treaty with ratifications by only 66 countries worldwide.[95]

---

[92] Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?," 472.
[93] Soma and Muther, "Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?," 333, 346.
[94] Wall, *Cybercrime: The Transformation of Crime in the Information Age*, 162.
[95] Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice," 61.

While this lack of consensus may be partly attributed to the novelty of cybercrime, Goodman and Brenner clarify that the limited progress is rather the result of "the *rejection* of efforts to persuade nations to adopt consistent, comprehensive cybercrime laws." They elaborate that the lack of consensus may reflect broader philosophical differences between states regarding what conduct should be permissible online.[96] Due to these fundamental differences in opinion, a host country may more frequently deny requests for extradition or quasi-extradition in cases of transnational cybercrime. They may not believe the conduct should be illegal or is severe enough to warrant the punishment that the pursuing country would impose. This political barrier again heightens the need for unilateral alternatives.

It also differs from the experience of other transnational crimes, such as drug trafficking, certain terrorist acts, and foreign corruption. As discussed above, there have been multiple UN conventions related to these offenses, which have been enacted with near universal ratification. This widespread acceptance creates a legal and normative obligation for states to cooperate formally or informally with transnational investigations. This starkly contrasts with cybercrime where the lack of international consensus means that states face no universal obligation to cooperate in cross-border prosecutions. Consequently, host countries enjoy greater latitude to deny assistance, decreasing the probability that extradition or quasi-extradition will succeed and leaving pursuing countries with unilateral alternatives.

Furthermore, I contend that cooperation is less likely to be in the political interests of host countries given the greater incidence of state sponsorship. Rather than bringing perpetrators to justice, it may be in the host country's national interests to allow cybercrime to flourish. Shull notes that China particularly benefits from economic

[96] Goodman and Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace," 216.

espionage and the theft of trade secrets, which are perpetrated via cybercrime.[97] Similarly, host countries may benefit from cybercriminals depositing or spending the illicit proceeds in their jurisdiction.[98] States may also wish to create an environment for their citizens to learn and develop technological capabilities, such as hacking, without undue fear of criminal prosecution. In addition to this tacit approval of cybercrime, the political issues associated with bringing perpetrators to justice are only likely to increase as states turn to directly sponsoring these offenses.[99] They may either task cybercriminals with doing the state's bidding or use their own military and intelligence officials to launch cyberattacks.

It is important to note that for the purposes of this analysis, I solely focus on state sponsored cybercrime, not cyberespionage or cyberwarfare. I am examining state sponsored attacks on business and individuals that, for example, breach their networks, generate illicit proceeds, indiscriminately steal personal information, and/or pilfer valuable trade secrets to benefit corporate interests. I am not concerned with states' efforts to hack the government or military and intelligence apparatuses of rival powers in order to gain a strategic advantage. Such actions fall under the realm of traditional espionage and are not generally treated as criminal justice matters. Equally important, I do not include acts of cyberwarfare. This refers to government-directed cyberattacks to cause death or physical injury to citizens or the destruction of property, such as by compromising and disrupting critical infrastructure systems.[100] Cyberwarfare can also refer to attacks against an adversary during wartime to disable, damage, or destroy their information structures and achieve superiority in the conflict.[101]

---

[97] Shull, "Global Cybercrime: The Interplay of Politics and Law," 14.
[98] Goodman and Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace," 218.
[99] *See* "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," March 23, 2018; "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," July 13, 2018; "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations."
[100] "Cyberwarfare Module."
[101] Bernik and Pomerol, *Cybercrime and Cyberwarfare*, 68.

As cybercrime cases involving state sponsorship become more prevalent, extradition and quasi-extradition will become less useful mechanisms. Host countries will instead strive to protect their agents and proxies from prosecution. Based on the degree of harm that these well-funded and well-executed state sponsored attacks can cause, pursuing countries will be compelled to respond. Hence, they will increasingly apply unilateral alternatives to bring the perpetrators to justice.

State sponsorship is also more likely to be a barrier in cybercrime than other transnational crimes. For the same reason why host countries generally possess the political will to combat other cross-border offenses, they are less likely to approve of those forms of illicit conduct. They recognize that by allowing drug trafficking, terrorism, financial fraud, or corruption to flourish in their territory, they risk these crimes creating domestic harms. Consequently, there is a greater concern that the costs to permitting these offenses would outweigh the benefits. This contrasts with cybercrime where the damage can be limited to abroad. Other cross-border crimes also enjoy greater international consensus, which would create a higher normative cost for a state condoning or sponsoring such illegal conduct.

Despite these considerations, there can oftentimes be a close connection between drug traffickers or terrorists and certain host countries. In the case of the former, this connection predominantly stems from corruption. However, corruption is a concern common to various transnational crimes, particularly those that generate significant illicit proceeds like drug trafficking or cybercrime. Since cybercrime confronts government policies that endorse or actively sponsor these offenses on top of corruption, it faces further political barriers and a heightened need for unilateralism.

Similarly, only very few rogue states sponsor terrorism. Even then, the extent of state sponsorship is not the same as in cybercrime. Foreign powers are generally not

deploying their uniformed military and intelligence personnel abroad to launch terrorist attacks. Such provocative actions could be considered acts of war and trigger armed conflicts. This contrasts with cybercrime where states actively rely upon their military and intelligence officials to launch cyberattacks. Considering that states may more vigorously protect their own agents versus proxies, I theorize that the challenges of bringing state sponsored perpetrators to justice are therefore more pronounced for cybercrime as opposed to terrorism.

Overall, the above complications related to the facts of the case (e.g., the remote nature of cybercrime), applicable laws (e.g., jurisdictional conflicts, dual criminality requirements, and the political offense exception), and political considerations (e.g., a lack of political will and state sponsorship) collectively lead to the prediction that pursuing countries are more likely to employ unilateral alternatives over extradition and quasi-extradition in prosecutions of cybercrime than other transnational crimes.

3. RESEARCH METHODOLOGY

While the novelty of cybercrime and gaps in the existing literature offer exciting research opportunities, they also present a series of methodological challenges. Primarily, the lack of a well-developed theory in this space means that any study must engage in a combination of both theory building and theory testing. Additionally, cybercrime investigations, which often involve national security considerations, are a sensitive matter. This makes it difficult for any researcher to gain access to the information necessary to examine this phenomenon. Indeed, many indictments remain under seal, and there is little publicly available empirical data. This chapter sets forth how I sought to overcome these obstacles in order to answer my core research questions.

In an ideal world, we would run a natural experiment to determine how the usage of unilateral alternatives compares between types of transnational crime. Yet, assignment to the treatment group (cybercrime) is likely not as if random. The second-best option would be to run a regression analysis on observed data to compare the proportion of cases employing unilateral alternatives between cybercrime and other cross-border offenses. We could also use a regression analysis to determine which of the predicted challenges of cybercrime have a statistically significant impact on the application of unilateral alternatives. However, there is no dataset that tracks the methods employed to secure custody over international fugitives. Furthermore, it is not always known from court documents or public reporting which obstacles were present in a given case and whether they influenced the deployment of unilateral tools.

As a result of these challenges, I employed a qualitative research approach of interviews and case studies. Specifically, I interviewed 81 current and former US federal prosecutors and agents as well as ten foreign officials from eight countries. The interviews provided the type of rich, deep explanations to both test the hypothesis and theory

developed in the previous chapter as well as identify additional explanatory factors affecting the use of unilateral alternatives. The case studies functioned as a further form of theory testing to determine whether the explanatory factors that emerged from the interviews have manifested in cybercrime prosecutions involving unilateral alternatives.

Indeed, interviews and case studies are largely anecdotal in nature and subject to the limitations of human memory and cognitive biases. Thus, they cannot definitively establish whether there are differences between the use of unilateral alternatives in cybercrime versus other transnational crimes or what factors drive these differences. However, the totality of the evidence, synthesized from conversations with many law enforcement officials and public records, ultimately provided a compelling narrative that shed light on both core research questions.

For the first set of interviews, I focused on speaking with prosecutors and federal agents who held leadership positions at the US Department of Justice (USDOJ), Federal Bureau of Investigation (FBI), Secret Service, and Homeland Security Investigations (HSI). This included one Deputy Attorney General (DAG, second-in-command of USDOJ), six Assistant Attorneys General (AAGs) who oversaw either the Criminal or National Security Division, the third-in-commands of both the FBI and Secret Service, and the Deputy Assistant Director of HSI's Cyber Division. Given their oversight roles, these individuals could offer the most holistic view of nationwide efforts and were best equipped to compare between cybercrime and other transnational crimes. I also spoke with prosecutors in key US Attorney's Offices to cross-reference the observations from headquarters and determine whether they matched the reality on the ground.

The vast majority of interviews took place in August and September 2019 in Washington, DC and New York, NY with additional interviews subsequently conducted via phone and video call. Each interview lasted between thirty and ninety minutes and

followed a semi-structured interview protocol, which was iteratively reviewed and updated based on previous interviews.

The case studies were determined by reviewing all USDOJ press releases of cybercrime prosecutions since 2000 and cross-referencing with media reporting to determine if a unilateral alternative was employed. I then contacted the specific federal prosecutors and, where known, agents involved in the case for interviews. The goal of these discussions was to determine why law enforcement resorted to a unilateral alternative. I triangulated these responses with court documents, press reports, and in some cases, books that were written on the cases to determine their reliability.

Throughout both sets of interviews, an emphasis was placed on adherence to the highest standards of research ethics. The interviews did not seek to illicit any classified information or specific law enforcement tactics. They also focused on closed cases. However, criminal investigations are still a sensitive topic. So, interviewees could face repercussions if they did not receive proper permission from their agencies to speak with me or revealed nonpublic information.

Therefore, I pursued ethics approval through the University of Oxford's Central University Research Ethics Committee (CUREC) process. I strictly followed informed consent procedures and offered all participants the option to have their responses pseudonymized. This ensured that participation in the study and responses could not be linked to any specific individual. In fact, pseudonymization facilitated open and honest discussions with interviewees since they did not fear their answers being traced back to them.

Upon completion of these interviews, all notes and audio recordings were transcribed and coded for data analysis. The primary codes were derived from the trichotomy of factual, legal, and political challenges expounded in the previous chapter.

New codes were added during the data analysis to capture additional explanatory factors that emerged during the interviews. Given the large number of interviews, coding assisted with digesting the results and comparing answers between respondents.

Despite the comprehensive nature of these results, the interviews predominantly involved US officials, who likely share a similar worldview. On the one hand, the US is the leader in investigating and prosecuting cross-border cybercrime, so it was logical to focus my research there. On the other hand, solely speaking with US officials might have presented an unduly positive view of US efforts or downplayed any US abuses of these criminal justice processes. Moreover, I brought my own biases as a researcher having worked for two summers at USDOJ, albeit on the issue of public corruption. Therefore, I sought to interview foreign law enforcement officials to further triangulate my findings. I also critically engaged with competing theories, such as the claim that the US is merely using lure operations to undermine the cyber talent of rival powers.

Finally, I explored the alternative hypothesis that any variation observed between cybercrime and other types of transnational crime is simply due to differences in the decision to investigate. In other words, the cases that law enforcement pursues in cybercrime may be systematically different than the cases pursued for other types of transnational crime. Since the decision to deploy a unilateral alternative is contingent on the preceding decision to investigate the case, such differences in the decision to investigate could then drive any differences observed in the use of unilateral action.

To address this alternative hypothesis, I probed the factors that underlie the decision to investigate through my interviews and compared the responses between prosecutors who specialized in cybercrime versus other key areas of transnational crime. I found no substantive difference in this decision-making process. This mitigates against the alternative hypothesis. Additionally, it provides greater reliability to the interview

evidence that fundamental differences indeed exist between the methods used to secure custody over cybercriminals as compared to other transnational criminals.

This chapter proceeds along the following roadmap. In the first section, I outline my rationale for the qualitative research approach of interviews and case studies. In the second section, I discuss the implementation of the comparative interviews, including participant selection, recruitment, and questioning strategy. In the third section, I review elements of the case study implementation, such as case selection and data collection. In the fourth section, I explain the research ethics considerations and steps taken to protect participants from any adverse consequences. In the fifth section, I detail my approach to data analysis and interview coding. In the sixth section, I summarize potential biases in my data sources and how I sought to mitigate these concerns. In the final section, I address the alternative hypothesis that differences in the decision to investigate cybercrime cases may in fact be what drives any differences in the use of unilateral alternatives.

3.1 Qualitative Approach: Comparative Interviews and Case Studies

Given the lack of adequate quantitative data, lack of established theories, and need for deep explanations, I employed a qualitative approach. This consisted of two parts: comparative elite interviews with US law enforcement officials and case studies of US cybercrime prosecutions involving unilateral alternatives. In the paragraphs that follow, I explain why I have focused on US practice in this area. I also detail the reasons why a quantitative research approach would not have been suitable for this analysis and the benefits of a qualitative approach. I then elaborate upon why specifically I turned to a combination of comparative elite interviews and case studies.

My analysis centered on US practice for several reasons. It was one of the first countries to introduce the use of unilateral alternatives to extradition as a recurring law enforcement tool, beginning in the 1970s as part of the War on Drugs. Furthermore, the

US has adopted a leading global role in the fight against transnational cybercrime due to its technical expertise in prosecuting such offenses. The complexity of these cases and limited investigative capacity worldwide means that the US is often one of the few venues where cybercriminals can be successfully brought to justice. In addition, the US has developed a robust global training program whereby cyber legal advisors are deployed around the world to inculcate best practices.[1] Based on this central position, the US is particularly interesting from a research perspective. Its efforts drive global law enforcement action on cybercrime. Through its training programs, the US may also encourage other countries to apply its tactics, such as alternatives to extradition. This suggests that my research findings may have broader applicability beyond the US.

The preferred method of testing the core hypothesis would have been to establish a data set consisting of all US prosecutions of transnational crime. I could have then run a regression analysis to determine if the use of unilateral alternatives to extradition is more likely for cybercrime cases than other transnational crimes. However, there is no US government dataset of the methods employed to secure custody over international fugitives nor is there a database that contains all indictments of transnational crime.

Alternatively, I could have searched USDOJ press releases to identify those transnational crime prosecutions involving extradition and its alternatives. Nevertheless, this process would have both faced feasibility concerns and likely generated a biased sample. While USDOJ's Computer Crime and Intellectual Property Section (CCIPS) maintains a comprehensive database of all cybercrime press releases since 2000, the same is not true for other types of transnational crimes. Additionally, it is not always made public through either the press release or subsequent media reporting how custody was secured. Even if this is mentioned, the explanation may omit important information. For

[1] "Overseas Work."

example, a press release may state that a Russian cybercriminal was arrested in Greece. Yet, this does not explain how the cybercriminal arrived in Greece. He could have travelled there on his own or been lured there.

Furthermore, most cases do not receive a press release unless there is an arrest or conviction. The likelihood of an arrest or conviction could be different for cases involving unilateral versus non-unilateral methods based on the type of crime. Plus, this data collection approach would not include cases where a unilateral alternative was attempted and failed, which could further bias the results. In other words, it could be that unilateral alternatives are employed more often in cybercrime cases but also fail more often in cybercrime. Thus, a data collection strategy relying on press releases could make it appear that unilateral alternatives are applied less in cybercrime when this is not the case.

Another more innovative quantitative approach that could have been applied to test this dissertation's hypothesis is a factorial survey. In this method, respondents are presented with hypothetical vignettes and a key factor, such as the type of transnational crime, is randomly varied. After each vignette, respondents rank on a Likert scale the likelihood of a certain outcome, in this case whether a unilateral alternative would be applied. Indeed, a factorial survey was a component of my initial research plan.

However, through my interviews, I discovered that most USDOJ prosecutors, with the exception of a few officials in leadership positions, tend to specialize in one area of crime. This means they do not often have substantial experience prosecuting other offenses. As a result, if a career drug trafficking prosecutor were presented with a vignette involving a cybercrime, their answer may have simply been an educated guess, limiting the value of this approach. A factorial survey also would not have provided any explanation behind the relationships that it may have uncovered. It would not have

revealed why unilateral alternatives may or may not be used more often in cybercrime or what factors influence their use in cyber cases.

This last element is particularly important considering the lack of existing theory in cybercrime. As described in the previous chapter, little has been written on the methods used to secure custody over international cybercriminals. Nor has there been any significant academic research on the factors that influence the use of unilateral alternatives. Indeed, there has been some writing on the difficulties of prosecuting cross-border cybercrime, which formed the basis for my prediction that unilateral alternatives will be applied more frequently due to the trichotomy of factual, legal, and political challenges. However, that theory is far from fully developed. This dissertation therefore needed to engage in a combination of both theory testing and theory building.

To address the above limitations, this study heard directly from the law enforcement officials responsible for devising and approving alternatives to extradition. Such a qualitative approach is particularly valuable when a need exists to explain results. As Creswell and Plano Clark observe, "quantitative results can net general explanations for the relationships among variables, but the more detailed understanding of what the statistical tests or effect sizes actually mean is lacking."[2] Through interviews and case studies, a qualitative approach can overcome these shortcomings by providing the thick descriptions necessary to understand the "why" behind state behavior.

Specifically, in-depth interviews "can generate more points of inferential leverage."[3] As Layna Mosley describes:

> Interviews also allow the researcher to gather a much deeper set of responses: she can ask questions that allow for open-ended responses; if these responses generate additional queries, the researcher can ask these as follow-ups, probing more deeply into the actions and attitudes of respondents. Such follow-up questions can be

[2] Creswell and Plano Clark, *Designing and Conducting Mixed Methods Research*, 9.
[3] Mosley, "'Just Talk to People'? Interviews in Contemporary Political Science," 6.

> particularly enlightening when the respondent appears to hold contradictory views, or when the phenomenon of interest is multifaceted.[4]

The interviews for this dissertation first sought to determine whether unilateral alternatives are employed relatively more frequently for cybercrime versus other transnational crimes. This relied on speaking with supervisory law enforcement officials who have overseen prosecutions of multiple types of transnational crime and can thus compare between offenses. It also involved interviewing career cybercrime prosecutors and agents. If the respondents consistently indicated that unilateral alternatives are applied more frequently than extradition and quasi-extradition in cybercrime cases as compared to other transnational crimes, this would have provided support for my hypothesis. On the other hand, if they revealed that unilateral alternatives are used at approximately the same frequency or less often in cybercrime cases, this would have given cause to reject my hypothesis.

An additional goal of these conversations was "to develop an emergent theory" by examining the salience of the predicted explanatory factors related to the facts of the case, applicable laws, and political considerations while also identifying new variables.[5]

Nevertheless, "to properly comprehend the presence of a phenomenon (the dependent variable) … one should also study cases where that phenomenon is not present."[6] Therefore, to introduce such variation into this study, I also spoke with law enforcement officials who have specialized in other forms of transnational crime, namely terrorism, drug trafficking, fraud, foreign corruption, and export control and sanctions violations.[7] I then compared their insights on the methods used to secure custody and the

---

[4] Mosley, 6.
[5] Creswell and Plano Clark, *Designing and Conducting Mixed Methods Research*, 90.
[6] Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*, 243.
[7] I originally only planned to interview law enforcement officials who have worked on terrorism, drug trafficking, fraud, and foreign corruption cases. However, my initial interviewees suggested that I also look into export control and sanctions cases, so those crimes were added for comparison in the midst of fieldwork.

factors that influence the use of unilateral alternatives with the responses received from cybercrime officials. This enabled me to determine the extent to which the challenges are unique to cybercrime or faced by other forms of cross-border criminality.

To further shed light on my second research question regarding the factors that influence a state's decision to pursue a unilateral alternative in a cybercrime case, I employed a case study analysis. Gerring explains that "case studies, if well-constructed, may allow one to peer into the box of causality to locate the intermediate factors lying between some structural cause and its purported effect."[8] Given the limited literature on alternatives to extradition especially within the context of cybercrime, case studies are particularly strong tools for identifying undiscovered variables and developing new theories.[9] Moreover, case studies can provide greater "detail, richness, completeness, wholeness, or … degree of variance in an outcome that is accounted for by an explanation."[10]

In the case studies, I applied the method of process tracing in order to map the causal mechanisms that lead a state to pursue unilateral alternatives in cybercrime cases. Process tracing is particularly well-suited for answering this second research question since it "is Y-centered, which means that the researcher is interested in the many and complex causes of a specific outcome (Y) and not so much in the effects of a specific cause (X)."[11] Additionally, process tracing can more accurately explain real-world events and decisions by recognizing that outcomes result from the combination of multiple causes, multiple paths can lead to the same outcome (equifinality), and the same cause may have different effects in different environments.[12] Furthermore, process tracing

[8] Gerring, *Case Study Research: Principles and Practices*, 45.
[9] George and Bennett, *Case Studies and Theory Development in the Social Sciences*, 20.
[10] Gerring, *Case Study Research: Principles and Practices*, 49.
[11] Blatter and Haverland, *Designing Case Studies: Explanatory Approaches in Small-N Research*, 80.
[12] Blatter and Haverland, 80.

employs multiple data sources to reconstruct what occurred and systematically considers and rules out alternative explanations in order to develop a robust causal chain.

This process tracing was largely based on a second set of interviews with the specific USDOJ attorneys and federal agents who investigated and prosecuted the selected cases. These served as a form of confessional evidence: "explicit statements of actors in which they reveal why they acted the way they did. These statements can contain information about all elements of a full-fledged mechanism-based explanation: information about how the actor perceived the situation, … indications about driving motions, … and reflections about the anticipated consequences of specific actions."[13]

Oftentimes, the decision to deploy a unilateral alternative is an internal law enforcement process, which is not expounded in court documents. Indeed, in many cases, the use of a unilateral alternative may not be disclosed at all. The only way to understand these causal mechanisms is therefore by speaking with the law enforcement officials directly involved. Such interviews involved a mixture of theory-testing and theory-generating. I probed the salience of the factors related to the facts of the case, applicable laws, and political considerations as well as sought to elicit new independent variables that may form part of this causal mechanism.

Overall, I opted for this mix of comparative interviews and case studies in order to triangulate the results and provide greater internal validity. For instance, if prosecutors expounded certain factors that affect the application of unilateral alternatives and these factors played out in the case studies, this combination of methods would enhance confidence in the findings.

[13] Blatter and Haverland, 117–18.

3.2 Comparative Interview Implementation

The comparative elite interviews relied predominantly on a purposive sampling of current and former federal prosecutors and agents at headquarters in Washington, DC as well as at key field offices across the US. These individuals could offer the most holistic perspective on the use of unilateral alternatives across the country and between different types of crimes. Interviewees were recruited by culling multiple public databases for contact information and then emailing them. The interviews were mainly conducted in person and followed a semi-structured protocol. The goal was to create a conversational tone to facilitate candid dialogue while still ensuring that information was elicited related to each of the predicted explanatory factors. While the accuracy of this anecdotal evidence may be limited by the recall and honesty of the interviewees, I sought to mitigate these concerns by cross-referencing responses both within and between interviews.

As Leech et al. note, purposive sampling is particularly useful for this type of analysis: "If the interview subjects are not themselves the topic of the study, but rather are being used as expert sources of information about some other unit of analysis, random selection might not even be advisable. Instead the researcher would want to purposefully select the individuals who are likely to know the most about the topic and talk to them."[14]

Furthermore, it simply would not have been feasible to interview all federal prosecutors who have worked on transnational crime in each of the 93 US Attorney's Offices across the country.[15] Therefore, I focused on interviewing those based at the USDOJ headquarters known as Main Justice since they are the subject matter experts, consult on high-profile cases, and set Department-wide policy.

[14] Leech et al., "Lessons from the 'Lobbying and Policy Change' Project," 214.
[15] The US Attorney's Offices are the USDOJ field offices that prosecute the federal crimes which occur in a specific geographic area (e.g., the Southern District of New York).

Specifically, Deputy Attorneys General, AAGs, Deputy Assistant Attorneys General (DAAGs), and Section Chiefs are responsible for determining policy and must approve all extraordinary requests, such as alternatives to extradition. They not only possess a thorough understanding of the crime areas they oversee but also would know when unilateral tools are deployed. Since DAGs, AAGs, and DAAGs supervise prosecutions of multiple types of crime, they likewise have a broader perspective to comment on comparisons between offenses. Therefore, I sought to speak with current and former AAGs and DAAGs for USDOJ's Criminal Division and National Security Division. I also sought to speak with the Chiefs of CCIPS, the Narcotics and Dangerous Drugs Section, the Counterterrorism Section, the Fraud Section, and the Counterintelligence and Export Control Section.

Additionally, attorneys at the Office of International Affairs (OIA) at Main Justice must consult on all requests that involve international action, such as alternatives to extradition, from federal prosecutors across the country. Based on the centrality of their role, these attorneys would have a similarly holistic view of the comparative use of unilateral alternatives between different types of crime. As a result, they were included in the interview selection criteria as well.

In order to introduce variation and triangulate these interview results, I also endeavored to speak with prosecutors at US Attorney's Offices with significant experience prosecuting transnational crime, particularly cybercrime. These included the Southern District of New York, Western District of Pennsylvania, Eastern District of Virginia, District of Columbia, and Western District of Washington. Perceptions may differ between Main Justice and the field offices. For instance, attorneys at Main Justice may adopt a more legalistic or conservative approach to the use of unilateral alternatives whereas

prosecutors on the ground may adopt a more tactical or ambitious mindset. Consequently, I sought to cross-reference the observations from Main Justice with those in the field.

Moreover, prosecutors are not the only law enforcement officials involved in the decision to deploy unilateral alternatives. In fact, the idea for such unilateral tools often originates with the federal agents investigating the case. As a result, I also spoke with leaders at the main federal law enforcement agencies, namely the FBI, Secret Service, HSI, and Drug Enforcement Administration.

Indeed, I discovered through my interviews that these agencies differ in their approach to unilateral alternatives. For instance, one prosecutor explained to me, "The FBI especially post-Watergate has a very highly regulated set of investigatory guidelines that they have to follow whereas the Secret Service, not having had that history, has a little bit more autonomy to operate in terms of developing investigations … So, there's a cultural difference that comes from that."[16] Similarly, Secret Service Assistant Director for Investigations Michael D'Ambrosio noted, "Because of our integrated protective mission, we're going to go out, generally speaking, and prevent crime as opposed to letting it occur in order to arrest people."[17] While all the investigating agencies engage in unilateral alternatives, these observations suggested that the responses received from leaders at certain agencies may be more conservative than others. Thus, it was essential that I speak to all relevant agencies and triangulate their answers.

Given the broad temporal span of this research beginning in 2000, I also included former federal law enforcement officials in my sampling. This assisted me in determining whether there have been any changes over the past two decades in the use of unilateral alternatives to combat transnational crime. Equally important, former officials may be

[16] Prosecutor 22, interview.
[17] D'Ambrosio, interview.

more candid and forthcoming in interviews. They are less likely to need the permission of their agency to participate. They also have less to worry about in terms of accidentally compromising ongoing law enforcement operations or facing potential retribution from the government for providing undesirable or unfavorable answers.

I relied on a variety of data sources to identify the specific individuals who held the positions of interest identified above. The Congressional Directory, which is issued at least once every two years, contains the names of all USDOJ AAGs, DAAGs, and section Chiefs as well as leaders at the investigating agencies. I also cross-referenced this information with both the print and online versions of the Federal Yellow Book publication, which is issued yearly. I identified further contacts through LinkedIn by searching for terms like USDOJ, CCIPS, and OIA.

Many of the prospective interviewees had their contact information available either online or through the Federal Yellow Book. Some did not have specific contact information available, but their email addresses could be guessed since their organization followed the same format for all employees. For certain employers, the format was not consistent, which required multiple guesses and resulted in several emails bouncing back. If all these attempts failed, I then tried reaching out to the individuals via LinkedIn messaging. This was generally the least reliable and slowest method of contact.

In my initial email, I explained the purpose of the project, my previous experiences with USDOJ, and requested a 30-minute meeting. If participants did not respond to the first email, I typically sent a follow-up message one to two weeks later. Persistence tended to be fruitful as many interviewees responded after the second message. This may have been because the original message became lost in their inbox, they forgot to reply, or the second email demonstrated my seriousness and specific interest in interviewing them. In certain cases where I did not receive a response to my initial email, I asked an existing

contact at USDOJ who I knew was a shared connection on LinkedIn or who worked in the same office to facilitate an introduction. A federal prosecutor vouching for me in this way generally helped secure the interview.

In total, I contacted 151 law enforcement officials. Roughly half of the individuals (73) accepted my interview request, five said they would consider participating but an interview was never scheduled, 20 declined to participate, and the remaining 53 never responded. Out of the 73 who accepted my request, I ultimately did not interview six due to persistent scheduling conflicts that were not resolved by the time I reached a saturation point with my interviews. This interview recruitment data is summarized in Table 1 at the end of this chapter. Overall, there did not appear to be any systematic difference in those who did not respond or who declined to interview from those who participated. For instance, within the political appointees I interviewed (DAGs and AAGs), there was an equal proportion of officials from Republican and Democratic administrations represented.

The most common reasons across both current and former officials who declined to be interviewed were a concern over sharing sensitive law enforcement information, a belief that they did not have sufficient expertise to offer, or a too busy schedule. In some of these cases, the official kindly offered to introduce me to better suited individuals. This yielded helpful new connections and placed me in contact with several former prosecutors whose email addresses I could not independently locate.

Reasons for officials agreeing to partake in this dissertation may have included an interest in furthering academic research and the enjoyment of sharing one's experiences. Respondents may have also been more prone to say yes due to my previous experience at USDOJ and stated career goal of becoming a federal prosecutor. Consequently, they may have viewed me as less of a threat and the interview as a mentoring opportunity of sorts.

The majority of these interviews were conducted in-person at the interviewee's office or in nearby coffee shops in Washington, DC and New York, NY. These cities house or are proximate to the main federal districts for prosecuting transnational crime. I preferred to conduct interviews in-person since, as Layna Mosley explains, "first, virtual interviews lack much of the contextual information that can be important to interpreting interview data … Second, it is more difficult for the researcher to establish rapport with the subject from afar, and this can limit the depth and accuracy of the information offered."[18] It was particularly important that I establish this rapport considering the sensitivity of the topics being discussed and the hesitancy of many to participate.

Each interview followed a pre-drafted interview protocol. However, during the interview, I did not read the questions directly from the document but rather asked them in my own words. My goal was to create a conversational tone in order to build rapport and encourage candor. Indeed, I often began each interview by discussing my experience at USDOJ, career aspirations, and common connections. The intent was again to put the interviewee at ease and demonstrate to them that I was more of an insider than an outsider. I hoped that they would then view me as less of a threatening academic who was scrutinizing their actions and be more forthcoming in their responses.

Once I moved into the formal protocol, I first asked about the interviewee's experience in federal law enforcement. I then probed how they define cybercrime to ensure that we were discussing the same offenses given that there is no universally accepted definition of cybercrime. I proceeded to ask about the challenges of securing custody over the transnational criminals they have prosecuted, how custody was typically secured in those cases, their experience with unilateral alternatives, the approval process

[18] Mosley, "'Just Talk to People'? Interviews in Contemporary Political Science," 7–8.

for such tools, whether the use of these methods differs between cybercrime and other cross-border offenses, and why these alternatives have been applied.

The interview questions began general and open-ended so as not to influence the interviewee's responses. However, if they did not refer to a specific predicted explanatory factor, I included follow-up probes related to the trichotomy outlined in Chapter 2. I sought to guide these discussions through the lens of specific cases on which the law enforcement officials had worked. As Beckmann and Hall explain with respect to elite interviewing in Washington, DC, "gathering valid data is greatly facilitated by tailoring it to the respondent's work on actual cases."[19]

Nevertheless, in many instances, law enforcement officials were not willing to provide identifying details on specific cases since they could not recall which aspects were approved for public knowledge. Consequently, the conversation remained at the general level. Yet, my approach to questioning may have at least primed the interviewee to recall specific cases and thus answer more accurately with those experiences in mind.

This interview protocol had been pre-tested with two trusted prosecutors who I knew prior to this research. They provided honest feedback on the structure, comprehensibility, and flow of the protocol. I also iteratively revised the protocol throughout my fieldwork. Specifically, I added questions as new explanatory factors emerged from the interviews and altered some of the language. In early interviews, I noticed that law enforcement officials bristled at the term "unilateral alternatives" and subsequently became defensive, impeding candid responses. As a result, I simply began referring to these as "lures or captures," which had less of a pejorative connotation.

At the end of each interview, I asked participants if there were any other law enforcement officials with whom I should speak as part of this research. This question

[19] Beckmann and Hall, "Elite Interviewing in Washington, DC," 198.

introduced an element of snowball sampling to the study. It helped me to identify further contacts who may have been left out of the initial selection criteria. In these instances, I typically asked the interviewee if they would be willing to connect me with the individuals they recommended. These connections were then more likely to lead to positive responses, which enabled me to gain access to several key officials who had not responded to my cold emails. Additionally, this snowball sampling helped confirm that I was speaking to the correct individuals. This provided even greater confidence when multiple interviewees indicated that I should interview the same person.

By January 2020, I had conducted interviews with 66 federal prosecutors and agents. Each interview lasted between 30 and 90 minutes with most lasting approximately one hour. The vast majority were in person, but interviews with those located outside of Washington, New York, or New Jersey were conducted via phone or video call. By January, I had also reached a saturation point. That is to say, the information that I was hearing from interviewees was becoming repetitive, and the marginal value gained from each additional interview had rapidly diminished. Therefore, I decided to stop reaching out to further law enforcement officials and following up with those who had agreed to be interviewed but had previous scheduling conflicts.

Over 2020 and 2021, I conducted twelve follow-up interviews, which lasted 30 minutes on average, and one interview with a new federal prosecutor. The purpose of these conversations was to fill holes that emerged after completing my data analysis and receiving feedback on preliminary drafts from professors and peers. These interviews tended to be limited in scope and focus on specific issues, such as the geopolitical aspects of the US prosecuting state sponsored cybercriminals. I selected individuals for these additional conversations based on the relevance of their experience to the present question.

For example, to clarify certain aspects of the US's approach to terrorism cases, I reached out to all the terrorism prosecutors whom I had originally interviewed.

Despite the large number of interviews conducted, this still does not represent the entire universe of federal prosecutors and agents investigating transnational crime. Thus, it is possible that I missed certain contrary perspectives, meaning that this qualitative evidence remains suggestive rather than determinative. Additionally, interviews suffer from several unavoidable limitations despite my best efforts to mitigate. For instance, the constraints of human memory mean that law enforcement officials may not recall with full clarity or accuracy the details of cases from over two decades ago or the factors that went into various decisions, such as whether to use a unilateral alternative.

Moreover, any such recollections may be subject to cognitive biases. The recency bias means that interviewees may be more likely to recall recent cases than historic ones. This may be problematic if the challenges of securing custody or use of unilateral alternatives have significantly changed over time. Likewise, the availability bias means that individuals tend to believe the examples that first come to mind are representative. However, this may not be the case since the first examples that come to mind may be the most extreme or anomalous ones, which is why they are remembered more easily.

There is also the concern that interviewees may simply lie or misrepresent information to make themselves or their organizations look better. This potential issue was easier to address for the in-person interviews. Layna Mosley explains that "an interview researcher knows not only what a respondent says, but also how the respondent behaved during the interview, whether the respondent hesitated in answering some questions more than others, and the context in which the interview took place. This metadata facilitates more accurate use and interpretation of interview data…"[20] In other words, it is possible to

[20] Mosley, "'Just Talk to People'? Interviews in Contemporary Political Science."

assess whether an interviewee is behaving candidly in an interview by observing their body language, changes in tone and demeanor, and other mannerisms, particularly when compared to their responses to earlier baseline questions.

Additionally, I relied upon on a strategy of triangulation to address the above weaknesses in the interview approach. Primarily, given the large number of interviews, I was able to compare responses between participants. When multiple officials expressed the same or similar views, this increased confidence in their observations. This was particularly true when responses were repeated across different groups of interviewees (e.g., Main Justice vs. US Attorney's Office, prosecutor vs. federal agent, FBI vs. Secret Service vs. HSI, etc.) or party affiliation for those officials who were political appointees. Indeed, I did not detect any variations in response based on political party.

As Jonathan Lusthaus details, triangulation can also occur within an interview:

> If something that has been said conflicts with what is known from existing data, the relevant topic can be raised more directly. If the subject continues to display good confidence in the account, it is at least clear they believe it with certainty. This means that the area might require further investigation to harmonize or otherwise resolve the conflicting data points. If the participant quickly backtracks from a point when questioned directly on it, then one knows to view it with caution, and might privilege other more credible data over these claims.[21]

In my interviews, I often raised similar questions multiple times but from different angles or with different wording to determine if the respondent would maintain the same answer. I also followed Lusthaus's recommendation of probing on responses that seemed to contradict information from earlier in the conversation or other interviews. If the contradiction could not be resolved, I added this as topic of discussion with future interviewees to ascertain whether others agreed with the point or it should be discounted. Finally, where possible, I sought to verify the information gleaned from the interviews

[21] Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*, 241.

with media reporting and public records to determine their consistency. This was a particularly useful strategy when officials referred to specific cases.

3.3 Case Study Implementation

For the case studies, I compiled a dataset of US cybercrime prosecutions involving unilateral alternatives. These cases were identified through USDOJ press releases, my initial comparative interviews, and media reporting. While there is a risk that I overlooked certain prosecutions, this did not impact my ability to establish the causal mechanisms within the identified cases. To determine such causal chains, I interviewed the prosecutors and agents involved, following a similar recruitment and questioning strategy as for the comparative interviews. I then cross-referenced these findings with media reporting and court records.

An analysis of all USDOJ press releases on transnational cybercrime in the CCIPS database from 2000 (the starting point of the database) through 2020 revealed 83 US prosecutions of cybercrime involving extradition and its alternatives. I then reviewed the press releases to determine how custody was secured over the perpetrator. Frequently, this was not explicitly stated, so I cross-referenced with media reporting. For instance, many press releases simply stated where the defendant was arrested. Likewise, the press releases did not reveal whether the offender was formally extradited or informally rendered through a quasi-extradition. Media reporting sometimes provided the answers, but this was not always the case.

Consequently, I was faced with the same challenge discussed earlier in this chapter that not all unilateral alternatives are made public. Therefore, this case selection strategy may have missed certain prosecutions that involved unilateral alternatives, which could have biased my results. I attempted to mitigate this concern by asking the officials I spoke with for the comparative interviews if there were any specific cases involving unilateral

alternatives that I should study. This strategy did identify a new case that I was not previously aware of but could not fully eliminate the risk of missing cases.

The secretive nature of how custody is secured in certain prosecutions has also led to media speculation and incorrect reporting. For instance, Maksym Yastremskiy was one of the world's most prolific carders (a hacker who steals payment card information). As part of their investigation into this Ukrainian cybercriminal, the Secret Service embedded an undercover agent. The agent had multiple meetings with Yastremskiy, including one in Turkey where Yastremskiy was arrested by local authorities at the request of the US government. In response to this arrest, prominent media organizations, such as Wired, reported that Yastremskiy may have been lured to Turkey.[22] However, I learned from my interviews that Yastremskiy's arrest was not the result of a lure. The undercover Secret Service agent and Yastremskiy frequently invited each other places, but this meeting was initiated by Yastremskiy rather than the agent.[23] This was the only such case I found where media reporting inaccurately suggested there was a unilateral alternative.

Another concern with my case selection approach is that it would not include cases where unilateral alternatives were attempted and failed, which are still relevant for my research questions. I again attempted to address this concern by searching news databases for media reporting regarding cybercrime cases with attempted lure or capture operations. I was able to locate an additional case, but again there is the likelihood that unilateral tools have been covertly tried in other cybercrime cases and failed.

Altogether, these limitations mean that readers should remain circumspect with respect to the external validity of the case studies. Nevertheless, the case studies still enabled me to robustly investigate the causal mechanisms that led to the use of unilateral

[22] Zetter, "Ukrainian Carding King 'Maksik' Was Lured to Arrest."
[23] Federal Agent 12, interview, February 12, 2020.

tools in the identified prosecutions. The imperfections of the case selection method do not change those findings or detract from the internal validity.

Indeed, since process tracing is interested in explaining the causes which lead to a given outcome, I focused my analysis on those twelve positive cases (cybercrime prosecutions that involved unilateral alternatives).[24] The positive cases were dispersed across the entire previous two decades, allowing me to account for any temporal effects. Additionally, the cases varied in terms of the nationality of the defendant, federal district in which they were prosecuted, and type of cybercrime, which enabled me to address those possible confounding factors. Specifically, the variations permitted me to make comparisons based on the subtype of cybercrime. Within the cases that I had sufficient data to analyze, the subtype of cybercrime did not appear to impact the need for a unilateral alternative or the likelihood that such a tool would be employed.

For the case study interviews, I once again employed both purposive and snowball sampling. As Cathie Jo Martin explains, "When constructing a case study to investigate causality in a particular case, one looks for the smoking gun: one cares less about getting a representative sample of the individuals who may have been affected by an event than about identifying the individuals or institutions responsible for causing the particular action."[25] Indeed, Beckman and Hall agree that "the people who worked on a particular bill, rule, appointee, or case know exceedingly well their actions in that specific context."[26]

Therefore, I focused on speaking with the specific law enforcement officials who worked on each of the case studies. I included both prosecutors and agents since they may have different perspectives or interpretations of events, which are important to cross-

[24] Blatter and Haverland, *Designing Case Studies: Explanatory Approaches in Small-N Research*, 100–101.
[25] Martin, "Crafting Interviews to Capture Cause and Effect," 113.
[26] Beckmann and Hall, "Elite Interviewing in Washington, DC," 198.

reference. To identify the prosecutors who litigated the case, I culled the press releases as well as the attorney list from the US federal courts PACER database. If the case involved a criminal complaint that could be accessed through PACER, the case agent's name was also listed. However, this was not always the case, so I then relied on snowball sampling by asking the prosecutors to identify or connect me with the case agents.

In total, I contacted 40 prosecutors and agents, of which fourteen agreed to be interviewed, five declined to interview, and the remaining twenty-one never responded. One prosecutor who agreed to speak with me was ultimately not interviewed due to persistent scheduling issues. This recruitment data is summarized in Table 1 at the end of this chapter. Overall, I was able to interview law enforcement officials who worked on nine of the twelve cases in question. There appeared to be no systematic difference in those who responded versus those who did not. The covered cases spanned the entire time period in question as well as involved multiple federal districts and various types of cybercrime. Therefore, there did not appear to be any significant non-response bias.

These interviews were conducted similarly to the comparative interviews, involving a semi-structured protocol and emphasis on creating a conversational tone. When the officials were in Washington, New York, New Jersey, or Pennsylvania, I conducted the interviews in person. All other interviews were conducted via telephone. The interview protocol began generally, asking participants about their background, definition of cybercrime, the challenges of securing custody over these offenders, and their experiences with extradition and its alternatives. I then turned to the specific case and asked the official to walk me through how custody was secured and why this approach was taken. Employing the logic of process tracing, I sought to rule out alternative hypothesis by probing on each of the explanatory factors that emerged from my theory and the comparative interviews.

I then endeavored to triangulate these responses by reviewing court documents (such as sentencing memoranda) and media reporting. In fact, the prosecutors involved in two of the cases wrote books on them. This allowed me to cross-reference their responses during the interview to ensure they were consistent with what they had written in their books, providing greater reliability and credibility to their words. Throughout my review of the court and media documents, I again applied the logic of process tracing to attempt to determine what factors influenced the use of unilateralism and systematically rule out alternative explanations.

3.4 Research Ethics Considerations

Given that this study involved human subjects, the highest standards of research ethics were applied to protect interviewees from any adverse consequences or risks of participating. This involved seeking approval from the Blavatnik School of Government Departmental Research Ethics Committee as part of Oxford's CUREC process. Additionally, each interview began with informed consent procedures whereby participants were asked to sign a consent form or provide their consent orally. Interviews were only audio recorded if the participant explicitly agreed, and their responses were pseudonymized to prevent the information they shared from being traced back to them.

The main risk to participants was that they were commenting on federal prosecution policies and practices, which can be a sensitive topic. Therefore, if they disclosed confidential or classified information, they could face repercussions from the US government, even if they were a former employee.

However, as current or former law enforcement officials, the respondents were experienced in handling sensitive information. This means they were well-aware of what they could and could not disclose, mitigating the risks of them accidentally sharing confidential information. Additionally, I took various steps to protect the participants.

They were all fully informed of the research ethics considerations. In my initial email contact, I included the project information sheet and consent form, which outlined the risks of the study and their rights as participants. I also reviewed these at the beginning of each interview, ensuring that officials understood their participation was voluntary and could be withdrawn at any time. I then presented each interviewee with a written consent form to sign before I asked my first questions.

Over the course of the research, I noticed that the written consent form unsettled certain officials. Some felt uncomfortable signing the document, particularly if their organization had not reviewed and approved the form. In fact, one official informed me that he could not to participate if required to sign the consent form. Consequently, I sought and received approval from the Blavatnik School to use oral consent instead, depending on participant's preference. Oral consent was still documented using a Researcher Record of Oral Consent form, but this did not require the interviewee's signature. As a result, subsequent participants seemed significantly more at ease. This appeared to facilitate open conversation since it did not cause interviewees to become guarded at the outset. Indeed, if I had used an oral consent process from the beginning, it may have led to more fruitful initial interviews.

To further protect participants, all interview data was pseudonymized using a generic code by default. On the one hand, pseudonymization provided interviewees with the flexibility to participate in the research and speak candidly. However, it also meant that I could not disclose any details regarding the interviewee's experience, such as years of government service or positions held, which would lend greater credibility to their observations. Some participants agreed to be quoted directly by name, which mitigated this limitation.

For those pseudonymized interviews, most participants were referred to as Prosecutor X or Federal Agent X. Some interviewees requested an even more generic pseudonym of Law Enforcement Official X, which was granted. Each code was randomly assigned to the interviewee. All calendar entries, notes, recordings, and transcriptions were labelled using the pseudonym. The only document linking pseudonym to real-identity was a password-protected, encrypted Excel spreadsheet, which was stored separately from the interview notes and transcriptions. When quoting from the interviews, I also omitted any details or comments that could identify the participant, such as a reference to a specific work experience.

Additionally, participants were given the option as to whether they wished to be audio recorded during the interview. On the one hand, audio recording facilitated the fluidity of the conversation since I was not preoccupied with capturing all the official's observations in my notes. It also allowed me to reproduce much richer and more detailed quotes in the chapters that follow. On the other hand, relying only on hand-written notes oftentimes encouraged the interviewees to be speak more openly and honestly about their experiences. Overall, it is unclear which option was more effective, but the decision ultimately laid with the participant.

One final research ethics consideration was that many participants requested to approve any quotes or paraphrases, even if pseudonymized, prior to publishing. These requests were uniformly granted and proceeded seamlessly. I was initially concerned that interviewees might use this opportunity to walk back potentially controversial statements that they made during our conversation. However, when officials suggested edits, it was either to clarify the message or strengthen the initial claim. This ability for interviewees to subsequently review their statements therefore appeared to only have had beneficial impacts in leading to more candid discussions.

3.5 Data Analysis

Upon conclusion of my fieldwork and return to Oxford, I transcribed all interview notes and audio recordings. The purpose was to enable coding of the interviews and facilitate comparing responses between officials. The codes were based on the predicted explanatory factors as well as new considerations that emerged from the interviews. This assisted in both the theory testing and theory development aspects of this research.

I manually transcribed my field notes but used the NVivo transcription service to transcribe the audio recordings given the sheer quantity and length of time covered. The NVivo transcription service did not produce perfect reproductions, particularly for interviews that occurred in public spaces like coffee shops or cafes. As a result, I needed to review and revise each transcript to ensure accuracy. However, this still saved a significant amount of time compared to personally transcribing each one.

I then developed a series of codes to analyze each transcript. The preliminary set of codes was based on the predicted explanatory factors related to the facts of the case, applicable laws, and political considerations. For instance, I created a catchall code of "applicable laws" and then subcodes of "dual criminality," "political offense," "jurisdictional conflicts," etc. During my fieldwork, I maintained a rough document listing the key findings from my conversations and particularly compelling quotes, which I continually updated. Therefore, I created additional codes based on new topics, such as the attribution challenge, that emerged from this initial rough analysis. Finally, I added codes as I analyzed the data and noticed further considerations that were relevant to my research questions. One example related to the use of unilateral alternatives to disrupt or deter cybercriminal conspiracies by sowing distrust.

Considering that this research involved both theory testing and theory development, the coding process enabled me to determine how the interviews and case

studies corresponded to the various elements of my theory. Furthermore, it permitted me to identify new casual variables of interest as new codes emerged from my data analysis.

Coding the data also greatly assisted with the cross-interview triangulation described earlier in this chapter. I was able to compare how various officials discussed key issues and identify how many times a topic was referenced. The more frequently a point was raised, the more likely it was to be a salient consideration. Consequently, when I found that responses were largely consistent between interviewees and that many officials referred to the same obstacle, this provided me with greater confidence in the finding. When I found that responses contradicted each other or that only a few officials raised a given point, this generally limited the confidence with which I could make a claim.

3.6 Potential Biases in the Data

My research focused on US efforts and relied on speaking with US officials. This means that my evidence predominantly stemmed from officials who likely share a similar worldview or perspective on these issues, potentially skewing my results. To mitigate this concern, I sought to speak with officials from other countries to cross-reference these observations. My international interviews followed the same semi-structured protocol and research ethics safeguards as the comparative interviews with US officials.

To elaborate upon the potential biases, US officials may present an unduly positive view of US efforts or downplay any abuses of process. For instance, the increasing interplay between nation-state activity and cybercrime may mean that the US is simply using lure operations to undermine the cyber talent of rival states. US prosecutors would likely have incentives to downplay such uses of the criminal justice tools, potentially biasing my results. Additionally, US law enforcement officials may raise issues that are unique to the US and not experienced by other countries, limiting the generalizability of my findings.

Moreover, I brought my own biases as a researcher to this analysis. I spent two summers interning at the Public Integrity Section of USDOJ, where I worked closely with federal prosecutors and agents on public corruption cases. I also plan to pursue a career as a federal prosecutor. While my experiences at USDOJ covered a different area of crime, I was still influenced by the Department's culture and norms. This socialization, in turn, could have impacted my analysis or interpretation of the data.

Consequently, throughout the research, I made a particular effort to cross-reference and verify findings wherever possible. As previously described, this involved asking questions multiple ways during an interview to determine if officials' responses remained consistent and checking their observations against public records, such as media reporting. I also critically engaged with competing theories, namely the claim that the US is simply applying lure operations for geopolitical purposes. Specifically, I scheduled several follow-up interviews with key prosecutors to press them on this question. While they provided reasonable defenses, I again did not simply accept their word but rather compared their claims against the empirical case record. This verification ultimately supported their accounts, providing a greater degree of reliability and confidence.

In addition, I sought to incorporate the perspectives of other countries to determine whether they were in accordance with the US view of cross-border cybercrime. For certain prominent cyber cases, particularly those involving state sponsored activity, other nations have issued public statements. Therefore, I was able to compare their response to the US position, which were largely consistent. Their statements further supported the claim advanced by US officials that the US is only prosecuting state sponsored cyber activity that crosses the acceptable bounds of cyberespionage.

However, these public statements generally occur only for the most substantial cybercrimes involving nation-state actors. Thus, this does not indicate whether other

countries have a similar experience or view to the US on prosecuting profit-motivated cybercrimes. Consequently, I endeavored to speak with foreign law enforcement officials. Not knowing the structure of foreign law enforcement agencies, it was difficult for me to determine who would be the correct or most knowledgeable official to speak with. Even if I could identify a potential interviewee, it would likely have been a challenge to gain access to them since my law enforcement connections were limited to the US. Thus, I had limited contacts to facilitate an introduction, and my cold emails might have remained unanswered.

Nevertheless, in November 2019, I attended the Council of Europe (CoE) Octopus Conference on Cooperation Against Cybercrime. This conference brought together all the member-states of the CoE Convention on Cybercrime, all states in the process of accession, and all states that have been invited to accede. Representatives from these countries generally included their lead cybercrime prosecutors, police, and investigators, precisely the individuals I was hoping to interview. Indeed, as Asif Efrat notes, "international conferences offer [International Relations] researchers a unique opportunity for face-to-face interviews with a large, cross-national group of actors who are involved in the political process under study."[27]

Prior to my arrival at the conference, I reviewed the list of attendees to preliminarily narrow down who would be most useful for my research based on their position and home country. Specifically, I focused on law enforcement officials from countries with an established reputation for prosecuting cross-border cybercrime. During the conference, I sought to meet these individuals. My goal was not to conduct an interview during the conference due to the limited time available between sessions but

[27] Efrat, "Cross-National Interviewing at International Conferences: How to Make the Most of a Unique Research Opportunity," 303.

rather to recruit them to participate in a subsequent phone or video call interview. In certain instances, the official in attendance did not believe they had sufficient experience or expertise to speak to my research questions but offered to introduce me to another official from their country. This still accomplished my objective. Given the large number of attendees at the conference, I was not able to meet everyone who I wanted to interview. However, I at least knew who to contact and had their email addresses from the attendee list, so I sent several cold emails upon my return to Oxford.

In total, I interviewed ten law enforcement officials from Belgium, Brazil, Israel, Germany, the Netherlands, New Zealand, Norway (via email), and the United Kingdom. Some of these connections were made after the Octopus Conference by reviewing attendee lists from previous years. I followed roughly the same interview protocol as the comparative interviews but removed any references to the US. I also followed the same research ethics procedures, reviewing the informed consent procedures and documenting oral consent via the requisite form. Four of the officials agreed to be quoted directly by name although two requested to approve any citations. The others agreed to be quoted pseudonymously simply by their country and general position or for the information to be used on background. Overall, the responses from these foreign law enforcement officials supported the observations from my US interviewees, particularly on the challenges of attribution and state sponsorship. More complete findings from these conversations are reported in the chapters that follow.

3.7 Alternative Hypothesis Related to the Decision to Investigate

Since a core component of this study involved comparing the use of unilateral alternatives between types of transnational crime, I also considered whether there are any systematic differences in the preceding decision to investigate these cases. Such a distinction could introduce a bias into the results since the decision to pursue unilateral

action is conditional on the decision to investigate the case. However, my interviews indicated that there is no fundamental difference in the decision to move forward with an investigation of a cybercrime versus other transnational crime. One prosecutor observed, "In my experience, there's no different approach as to whether we'll undertake the investigation."[28] Indeed, the factors that my interviewees most frequently identified in the decision to proceed with a cybercrime case are common to all transnational crimes.

Prosecutors regularly pointed to the Justice Manual (formerly known as the US Attorney's Manual), which outlines the Principles of Federal Prosecution.[29] These criteria, which prosecutors are supposed to consider in determining whether to move forward with a case, are designed to promote uniformity across the department and do not differ based on the type of crime. While the existence of such policies on paper do not guarantee they will be implemented as intended, the responses of prosecutors indicated that these guidelines are generally followed. Not only did the interviewees repeatedly refer to the Principles without prompting but also when asked to list the factors that they consider, the majority independently listed those outlined in the Justice Manual.

First, prosecutors indicated that they consider the nexus to the US. For cybercrime, this is typically an easy hurdle to overcome since, as one prosecutor explained, "if it passed through a US server of some sort, the reality is we have jurisdiction over it."[30] Given the breadth of US statutes, the prosecutor clarified that it is generally easy to satisfy jurisdictional requirements for "almost all [types of] crime."[31]

Next, prosecutors examine the degree of harm, which was cited as the most important criteria influencing the decision to pursue a case.[32] A prosecutor recounted to

[28] Prosecutor 29, interview, August 13, 2019.
[29] Prosecutor 4, interview, August 6, 2019; Prosecutor 13, interview; Rosenstein, interview.
[30] Prosecutor 17, interview.
[31] Prosecutor 17.
[32] Prosecutor 35, interview; Prosecutor 42, interview; Prosecutor 47, interview.

me, “It’s a question of ok, so, what was the impact to the United States, United States citizens or persons? Or alternatively, how big a global problem is this? … I think as a prosecutor you’re always asking that question. It really is the harm to US interests, citizens, corporations, the legal system.”[33]

Given the resources needed for cross-border cases, prosecutors likewise consider the size of the conspiracy and connection of the perpetrator to a pattern of recurring criminality. This enables the government to have the greatest impact within the constraints of its limited resources.[34] It also means they tend to focus their efforts on the leaders of the criminal conspiracy rather than low-ranking perpetrators.

Furthermore, prosecutors indicated that they evaluate the deterrent value of proceeding with the case. Specifically, they assess the broader media impact and potential public messaging associated with the case.[35] They similarly weigh the potential sanction and whether the crime will “merit a sentence that can reflect the seriousness.”[36] This is particularly relevant in determining whether a foreign partner or the US will prosecute since many other countries have weak sentencing that may not be appropriate for a recidivist or leader of a criminal network.[37]

The interviewed prosecutors did indicate that there may be certain distinctions in the individual decisions to proceed with cases given that these determinations are made by different attorneys. Since prosecutors at Main Justice typically specialize in one area of criminality, the attorneys deciding to move forward with a cybercrime case are different than those working on other types of transnational crime investigations. However, as one prosecutor clarified, this does not systematically skew which cases are pursued based on

[33] Prosecutor 17, interview.
[34] Prosecutor 23, interview.
[35] Prosecutor 27, interview.
[36] Prosecutor 14, interview.
[37] Prosecutor 55, interview.

the underlying offense.[38] In fact, USDOJ supervisors usually oversee multiple sections that specialize in different crimes to prevent any such fundamental differences.

Overall, the interviews indicate that the decision to pursue a cybercrime case does not differ in any meaningful way from other transnational crimes. None of the above cited factors are unique to cybercrime but rather are common to all transnational crimes. Therefore, this evidence mitigates against the alternative hypothesis that any observed differences in the use of unilateral alternatives are attributable to distinctions in the decision to pursue the case.

Table 1: Interview Recruitment Data by Type of Interview

Number of Officials	**Comparative Interviews**	**Case Studies**
Contacted	151	40
Did Not Respond	53	21
Declined	20	5
Maybe, Never Interviewed	5	0
Accepted, Never Interviewed	6	1
Accepted, Interviewed	67	13

[38] Prosecutor 28, interview, August 9, 2019.

4. THE CHALLENGES OF SECURING CUSTODY OVER INTERNATIONAL CYBERCRIMINALS

For weeks, Romanian cybercriminal Cezar Butu had been flirting online with a beautiful American woman. They had met while both traveling the previous year and hit it off. As an independently wealthy Hooters waitress, she soon invited him to visit her in the United States. However, when Butu stepped off the plane, he was not greeted by the attractive blonde he expected. Rather, he was greeted by US Secret Service agents and a pair of handcuffs. Little did Butu know, undercover law enforcement had lured him to the US. Their objective: to prosecute him for committing a multimillion-dollar hack and theft of payment card information.[1]

Though seemingly extraordinary, lure operations such as this are regular tools that US law enforcement employ to bring international cybercriminals to justice. In fact, I interviewed 81 US federal prosecutors and agents who have spent their careers tracking down transnational criminals. These officials had incentives to downplay the use of unilateral methods like lures due to their contested status under international law and potential diplomatic ramifications. Yet, they readily acknowledged their application. These conversations suggested that unilateral alternatives are employed more frequently in cybercrime cases as compared to other transnational crimes.

I learned that such unilateralism has only manifested in the form of lure operations for cybercrime. After all, cybercrime is a nonviolent offense, and a capture operation would thus not be worth the risk. However, as we will see in the next chapter, prosecutions of other transnational crimes have employed capture operations. So, my analysis and comparisons do not just focus on lures. Rather, I consider all unilateral alternatives.

[1] Krebs, "Alleged Romanian Subway Hackers Were Lured to US."

Why may unilateralism be more prevalent for cybercrime? I test the hypotheses that cybercrime presents challenges related to the facts of the case, applicable laws, and politics, all of which impede relying on formal or informal methods of cooperation. I find that barriers to cooperation do exist but are driven by the factual and political complications rather than legal obstacles.

Primarily, cybercriminals can hide from extradition behind the anonymity of the internet. A prosecutor confessed to me, "I can oftentimes know that a [specific] computer was involved. That's a far cry from knowing who the person at that keyboard was."[2] Law enforcement may not even know with certainty where the cybercriminal is located.

Yet, they must approach a specific country to request extradition. They must also prove that the individual in question committed the offense.[3] As a result, pursuing countries face a strong reason to resort to unilateralism in the form of a lure operation. Even if law enforcement does not definitively know where the perpetrator is located, they can communicate with him online and convince him to travel. Plus, once he falls for the ruse and arrives, it is difficult for him to credibly deny involvement.

The attribution challenge is compounded by cybercrime's remote nature. Perpetrators can strike from anywhere around the globe. Assistant Director for Investigations Michael D'Ambrosio, the third-in-command of the US Secret Service who has over 30 years of experience, elaborated to me, "The challenge obviously is … most other crimes at some point you will have gone to that nation and conducted the act, where[as with] cyber you may be conducting this act from wherever and never moved to that particular nation."[4] This not only precludes law enforcement from arresting

[2] Prosecutor 17, interview.
[3] Prosecutor 44, interview.
[4] D'Ambrosio, interview.

perpetrators within their territory but also allows cybercriminals to shelter indefinitely in safe haven countries.

But, why can't these host countries be relied upon to hand over or domestically prosecute cybercriminals? I predicted that cooperation would be blocked by a variety of legal barriers. However, my interviews with law enforcement officials revealed that legal obstacles do not meaningfully impede cooperation.

Extradition requires that the conduct be illegal in both countries, which I expected would be an obstacle for novel offenses like cybercrimes. Nevertheless, most countries have already enacted adequate cybercrime legislation. In fact, I learned from my interviews that the Council of Europe (CoE) Convention on Cybercrime (Budapest Convention) has been "an enormous blessing" in harmonizing cybercrime laws globally.[5]

When dual criminality barriers remain, prosecutors can charge the underlying offense, such as fraud, which enables extradition to proceed from a legal perspective. Additionally, the few countries that have not updated their laws are not home to high-profile cybercriminals. Therefore, these countries do not present a pressing challenge.

I also anticipated that state sponsored cybercriminals could successfully argue their actions are political offenses. These crimes would then be legally excluded from extradition. However, due to the commercial nature of cybercrime, I find that this defense rarely holds water.

Further, the US has solely focused on prosecuting cybercrimes that are profit-motivated or extend beyond the accepted bounds of cyberespionage, such as stealing proprietary data from private corporations. I found no evidence that the US is indicting cyber intrusions that are analogous to real-world espionage and that countries regularly engage in, like surveilling the military or intelligence apparatuses of rival powers.

[5] Kerkhofs, interview.

In fact, by working with global partners, the US is establishing international norms as to what state sponsored cyber activity crosses the line into criminal conduct. Hence, when perpetrators of these crimes are arrested in third countries, extradition has not failed on political offense grounds.

Despite these advancements, one legal barrier may remain: the pursuing country may lack an extradition treaty with the host country. Nevertheless, this challenge is not unique to cybercrime nor is it a death knell for cooperation. The pursuing country may negotiate an ad hoc agreement with the host country. Or, the host country can informally hand over the cybercriminal outside of the extradition process. Even if the host country's laws prohibit such forms of assistance, they can domestically prosecute the offender.

So, considering that legal complications do not significantly impede bringing cybercriminals to justice, why are perpetrators still able to shelter in certain countries? I discovered that host countries often lack the political will to cooperate in handing over these offenders. Local politicians recognize that they can score political victories by standing up to the pursuing country and refusing to assist. Taking a stand can be easier for cybercrime since perpetrators typically do not target victims in their own country or have any harmful domestic impacts. Moreover, cybercrime is still seen as largely non-violent.

I also learned that host countries may disagree as to the seriousness and wrongfulness of cybercrime. They "may not have as clear cut a view in terms of the morality associated with" this conduct as compared to other transnational crimes.[6] Furthermore, the perception of these offenders as the "kid next door" can generate greater public sympathy. These factors all undermine host countries' interest in assisting with an extradition or quasi-extradition, even among the US's longstanding allies.

[6] Prosecutor 23, interview.

Certain host countries, such as China, Iran, North Korea, and Russia, take this unwillingness to cooperate a step further by actively sheltering cybercriminals.[7] These offenders have a certain "motive or expertise to exploit" that such countries can use to accomplish policy objectives. For example, if they provide safe haven to cybercriminals, these countries believe that they can later task them with intelligence activities.[8]

The blending of the cyber threat in countries like China and Russia "can complicate things because most of their hackers, even if it's superficially completely criminal, have some connection to the governmental hacking apparatus. So, they've got an interest in keeping them out of the hands of rival countries."[9] Therefore, bringing these individuals to justice through extradition, informal cooperation, or domestic prosecution is usually off the table.

Even when cybercriminals travel and are arrested in third countries, state sponsors have successfully blocked extradition to the pursuing country. These nations have interfered by launching competing extradition requests, bribing public officials, and bringing diplomatic pressure to bear on the third country.

Given these factual and political challenges of cybercrime, what option is law enforcement left with to secure custody? Ferreting out cybercriminals using a lure operation. One prosecutor elaborated to me, "The people who are most adept at this are in places that we don't necessarily have the greatest relationships with or even have extradition treaties with, so you need to contemplate lures, inducements to travel, other sort of out of the box thinking … to get law enforcement's hands on these people."[10]

[7] Prosecutor 2, interview; Prosecutor 21, interview; Stigall, interview, August 15, 2019; Prosecutor 45, interview.
[8] Prosecutor 17, interview.
[9] Prosecutor 28, interview, August 9, 2019.
[10] Prosecutor 45, interview.

Securing physical custody is a particularly pressing concern here since cybercriminals can inflict unprecedented economic losses with virtually no limit on their ability to commit further crimes. This creates an urgency to arrest them and end their illicit conduct. Mary McCord, the former Acting Assistant Attorney General (AAG) of the National Security Division (NSD) of the US Department of Justice (USDOJ) and a career prosecutor, affirmed that "cyber cases are actually among cases that should be considered for lures because those actors are able to continue so easily their activity."[11]

Despite these findings, it is important to note that the role of state sponsorship here raises a viable alternative hypothesis that the use of unilateral alternatives is merely a cover for national security operations. The US may simply be launching lure operations to gain a geopolitical benefit by undermining the cyber capacity and incarcerating the most talented cyber actors of rival powers. Indeed, many countries treat cyber threats as a military, not law enforcement, matter. This hypothesis raises questions about the reliability of my interview subjects, who are all US government officials and likely represent a homogenous view of US policy. Their responses may seek to portray the US in the most positive light and vindicate its application of unilateral tools by overstating the challenges of cybercrime.

While it is impossible to truly divine the impetuses for US prosecutions and conclusively rule out these propositions, I find that several factors mitigate against the alternative hypothesis. As previously explained, the US has focused on prosecuting cyber cases that cross the lines of acceptable forms of cyberespionage as agreed upon by the international community. In fact, one of the most prolific offenders, China, has even assented to such norms against the state sponsored theft of trade secrets.

[11] McCord, interview, August 14, 2019. Mary McCord also served as Principal Deputy Assistant Attorney General of NSD and Chief of the Criminal Division of the US Attorney's Office for the District of Columbia.

Plus, the US is not a unitary actor but is rather composed of multiple government agencies with competing interests. Its national security institutions, which would be most interested in undermining the cyber talent of rival powers, have pushed back against using criminal prosecutions to combat state sponsored cyber threats. They prefer to monitor such cyber actors for intelligence purposes.[12] They are also deeply apprehensive about the risks of revealing sources and methods and tipping off state sponsors through criminal charges.[13] This explains why the US did not prosecute any state actors for cybercrime until 2014. However, USDOJ believes that any criminal conduct targeting US citizens and businesses should be prosecuted, which led to those first charges in 2014.[14]

Moreover, the use of unilateral alternatives by the US is not limited to cybercriminals residing in rival powers. These tools have been used against friendly countries when, for example, the attribution challenge has proved insurmountable or those countries lacked the political will to assist. In order words, the US is not solely targeting rival powers with unilateral alternatives.

To further address the alternative hypothesis and potential bias of my US interviewees, I spoke with ten officials from Belgium, Brazil, Germany, Israel, the Netherlands, New Zealand, Norway, and the United Kingdom. Their observations independently confirmed revelations from the US officials.

This chapter takes the following structure. The first section explores the methods used to secure custody over perpetrators of cross-border cybercrimes and probes whether unilateral alternatives are applied more frequently there. The second considers how the challenges of attributing cybercrimes impact the methods used to lay hands on these offenders. The third discusses the implications of cybercrime's remote nature. The fourth

[12] Prosecutor 28, interview, January 7, 2020.
[13] McCord, interview, August 6, 2020.
[14] Prosecutor 28, interview, August 9, 2019.

investigates whether legal factors, such as dual criminality requirements, the political offense exception, and jurisdictional conflicts, pose barriers in cybercrime cases. The fifth probes how the lack of political will in host countries impedes cooperation in cybercrime prosecutions. The sixth examines another political consideration: the role of state sponsorship. The seventh briefly summarizes the key findings of this chapter.

4.1 How to Secure Custody Over International Cybercriminals

In this section, I find that extradition, quasi-extradition, waiting for defendants to travel to the US or a cooperative third country, and lure operations have all been used to bring international cybercriminals to justice. However, so far, capture operations have not been deployed in these cases due to the risks involved. I also report and critically engage with the interview findings, which support the prediction that unilateral alternatives are applied more frequently in cybercrime cases as compared to other transnational crimes.

It's December 23, 2009 and you're US Homeland Security Investigations Special Agent Brendan Cullen. You've just walked into the pristine Pennsylvania offices of defense company Analytical Graphics Incorporated, expecting to give a boilerplate briefing on how to counter weapons and technology smuggling. However, you walk out with the beginnings of a case that over three years later will bring down a $100 million software pirate.

You've just learned of a website called CRACK99.com, which is selling thousands of pieces of high-tech software at incredible discounts. These products have been "cracked," meaning that the license files and access controls have been disabled or avoided. Disconcertingly, this software has a wide range of applications from defense to manufacturing to space exploration to aerospace simulation to explosive simulation. In the wrong hands, these products could pose a critical threat to US national security. After

launching a multi-year undercover investigation, you track the site back to Chengdu, China and identify its owner as a man named Xiang Li.

At first glance, the US may appear to be licking its lips here at the opportunity to constrain or undermine the military technological advances of its major rival. Indeed, the lead prosecutor on the case, former Assistant US Attorney (AUSA) Dave Hall, reflected to me, "The most important factor was that it was clear to me … and also to the agents that this case had an immediate national security implication."[15]

While these concerns undoubtedly prioritized the CRACK99 investigation, AUSA Hall noted that "this is an IP theft and … a criminal copyright violation … this is just a property theft case because that's really what [Xiang Li] was. He was a fence, selling stolen property."[16] After all, the case was brought to investigators by one of the victim companies, which was bleeding thousands of dollars in lost proceeds as its proprietary software was sold to customers around the world for pennies on the dollar. Additionally, the purchasers of this cracked software were not limited to China: over one-third were in the US. Investigators also found no evidence linking the perpetrator to the Chinese government. Although the stakes may have been higher given the applications of the cracked software, this case was no different than any other theft of intellectual property (IP), which is at its core a criminal matter.

Now, you, as Special Agent Cullen, are faced with the question: how do you bring this international cybercriminal to justice? Like many of the prosecutors and federal agents I interviewed, your initial instinct would likely be to pursue a formal extradition. In fact, prosecutors frequently remarked that this is their first preference. One cybercrime prosecutor explained that "if he is in a country where we can extradite him, then that's

[15] Hall, interview.
[16] Hall.

what we do."[17] A review of press releases for US prosecutions involving cybercriminals located abroad supports these observations that extradition remains the most frequent tool applied to secure custody.[18]

However, as is the case for any transnational crime, host countries do not always extradite as "a matter of practice."[19] They may not have an extradition treaty with the requesting country. This would have blocked extradition in the Xiang Li case since there is no such agreement between the US and China. Additionally, the host country's constitution may prohibit them from extraditing their citizens, which would have similarly blocked China from handing over Xiang Li. Host countries may also find other non-legal grounds to deny the request, even if they have friendly relations with the pursuing country.

Multiple prosecutors lamented the cases of Gary McKinnon and Lauri Love, both British nationals whose extradition was denied by the UK. McKinnon was indicted in 2002 for hacking into 92 computers in the US national security apparatus, deleting critical files, and stealing passwords in what prosecutors described as "egregious conduct."[20] However, another prosecutor explained, "After Gary's appeals and the like, British courts ordered him extradited, and Theresa May, who was Home Secretary at the time, … said no, he wasn't coming."[21]

Likewise, Love was charged with hacking into thousands of computer networks, including those of US military and government agencies. He stole confidential information, including personally identifiable information (PII) of government employees,

[17] Prosecutor 29, interview, August 13, 2019.
[18] See Chapter 3 for a methodological discussion on the limitations of the conclusions that can be drawn from examining the USDOJ press release archive.
[19] Prosecutor 42, interview.
[20] "London, England Hacker Indicted Under Computer Fraud and Abuse Act for Accessing Military Computers"; Prosecutor 2, interview.
[21] Prosecutor 29, interview, August 13, 2019.

and posted some of it on public websites.[22] One prosecutor elaborated that "he engaged in some pretty sophisticated and potentially damaging hacks."[23] His extradition was denied for the same reason as McKinnon's: both suffer from mental health issues and the UK was concerned for their human rights.

Given that extradition from the cybercriminal's home country is not guaranteed and would not have succeeded for Xiang Li, what would you consider next? Depending on the relationship with the host country, law enforcement may turn to a quasi-extradition. In this informal means of cooperation, the host country may simply hand over the cybercriminal or render him through a deportation or expulsion.

For instance, Russian cybercriminal Roman Seleznev was accused of hacking into the point-of-sale systems of restaurants and businesses to pilfer credit and debit card numbers. He and his co-conspirators then used this compromised information to steal millions of dollars. In July 2014, he was arrested in the Maldives. However, the US does not have an extradition agreement with the Maldives. So, the US negotiated with the government of the Maldives for them to deport Seleznev. Maldives police informed Seleznev that he needed to leave on the next available flight out of the country, which just so happened to be a Secret Service jet flying to the US territory of Guam.[24]

Nevertheless, a deportation or expulsion is only possible if the individual is not a citizen of the host country. Therefore, neither option would have succeeded for Xiang Li since he was a Chinese citizen. Additionally, the Chinese government likely would not have been interested in cooperating through an informal handover due to its state support for IP theft. AUSA Hall plainly observed, "In China, they encourage this."[25]

---

[22] "Alleged Hacker Indicted in New Jersey for Data Breach Conspiracy Targeting Government Agency Networks"; "U.K. Computer Hacker Charged in Manhattan Federal Court with Hacking into Federal Reserve Computer System."
[23] Prosecutor 45, interview.
[24] Law Enforcement Official 1, interview.
[25] Hall, interview.

Hall might have had an incentive to overstate this political challenge to justify not seeking China's assistance. Nevertheless, China has a long track record of state sponsored IP theft. Cybersecurity firms, such as FireEye and Mandiant, have attributed multiple cyber intrusions to pilfer trade secrets directly to the Chinese government and its proxies. In 2018, Australia, Canada, NZ, Japan, and the UK all joined the US in independently attributing a decade-long campaign of cyber-enabled IP theft to the Chinese Ministry of State Security.[26] Both these private sector and foreign government attributions corroborate China's support for the exact types of crimes in which Xiang Li engaged.

Continuing to move through the list of methods to secure custody over international cybercriminals, you may now consider tracking the offender's movements. If lucky, this would enable you to arrest him upon travelling to the US or a cooperative jurisdiction.[27] It's important to note that waiting for the defendant to travel is not considered an alternative to extradition since it occurs as a function of sheer fortuity. And, it generally still involves a formal extradition from the third country. Nevertheless, prosecutors shared with me that this approach has produced positive results:

> There have been some really successful prosecutions where an indictment is filed, and we just wait, and the people wind up travelling. There are a lot of cyber criminals who live in countries that are not as warm and as fun and have as many opportunities for spending money and enjoying the fruits of their criminal activity. So, they may travel for example from Eastern Europe to beaches of Thailand or to Amsterdam and elsewhere where they can then be extradited and have been extradited from there.[28]

For this strategy to succeed, prosecutors typically file the indictment under seal to avoid alerting the perpetrator. They then hope that the offender will risk travelling, believing that he has protected his anonymity.[29] If the defendant is located in a third country, the pursuing country may then seek a provisional arrest warrant (PAW). In other

[26] Cimpanu, "Five Other Countries Formally Accuse China of APT10 Hacking Spree."
[27] Weinstein, interview, August 6, 2019.
[28] Prosecutor 2, interview.
[29] Prosecutor 47, interview.

words, the pursuing country may urgently request that this third country apprehend the cybercriminal on the understanding that there will later be a full extradition request.[30]

PAWs have been increasingly used for intercepting cybercriminals. These individuals may only be in the third country for a short period of time, especially if on vacation. By the time that the pursuing law enforcement discovers his location, the perpetrator may be nearing the end of his visit. In the time it would take to process an extradition request, he may disappear again. However, a PAW mitigates this concern.[31]

For example, from March 2013 to January 2014, Vadim Polyakov stole personal information from StubHub users and resold thousands of pilfered e-tickets for major events.[32] Throughout the investigation, law enforcement took steps to monitor his whereabouts since Polyakov had two weaknesses. First, he was a car enthusiast who loved to travel internationally to watch races. Second, Polyakov and his contacts were active on social media. Thus, when one of his associates posted a picture of his feet up while lounging on a beach in Spain, law enforcement sprang into action. They noticed a third male foot in the photo and immediately wondered if it belonged to Polyakov. Chasing this lead, they called the hotel whose name was visible in another photo from the trip. The hotel confirmed that Polyakov was indeed a guest. Based on a PAW, Spanish authorities arrested him within 24 hours and formally extradited him eight months later.[33]

Like most other cybercriminals, Xiang Li nevertheless did not generally travel on his own, forestalling this wait and see approach. Left with no other alternatives, you, as Special Agent Cullen, might now consider a unilateral method to bring Xiang Li to justice. One such unilateral tool would be a capture operation. This alternative, which has been

[30] Prosecutor 29, interview, August 13, 2019.
[31] Prosecutor 29.
[32] "DA Vance: Ringleader of International Cyber Fraud Ring Sentenced to 4-to-12 Years in State Prison for StubHub E-Ticket Scheme."
[33] Law Enforcement Official 3, interview, September 25, 2019.

used for other types of transnational crime, would involve sending US law enforcement or military into the host country to directly arrest the defendant. The perpetrator would then be brought back to the US to stand trial.

However, this method has not been used for cybercrime cases. One prosecutor plainly stated, "at least in this area we're not sending agents into a country to grab him."[34] Simply put, the threat of cybercrime is not currently viewed as dire enough to justify risking the lives of American agents, breaching a country's sovereignty, and seizing one of their citizens. While prosecutors might have an incentive to conceal the use of capture operations, a review of all US transnational cybercrime prosecutions confirmed that not one involved this tool.

Yet, this does not eliminate the possibility that capture operations may be considered as the cyber threat evolves. AAG McCord outlined for me the conditions under which such a drastic step may be taken:

> I can't imagine doing [a capture operation] for cyber unless it's a cyberattack that resulted in death because that's a very extreme situation when you actually enter another country and capture one of their citizens and you really have limited circumstances where that would apply … If it was causing continuing significant harm particularly if that harm could involve personal bodily injury, then I wouldn't put it off the table.[35]

Since the cyber threat has not yet reached this threshold, especially in the CRACK99 case, you would be left with only one viable option to apprehend Xiang Li: a unilateral lure operation. In fact, this is precisely what the real Special Agent Cullen and his law enforcement partners pursued.

Using the ongoing undercover operation, they became loyal customers of Xiang Li and soon approached him with a business opportunity. He was selling the cracked software for far too cheap in the US. With their supposed connections, they would assist him with

[34] Prosecutor 28, interview, August 9, 2019.
[35] McCord, interview, August 14, 2019.

distributing the software in the US and boost his profits. But, the undercover agents told Xiang Li he would need to deliver the pirated software, design packaging, and 20 gigabytes of stolen data from a defense contractor to them in person. After negotiating possible meeting locations, Xiang Li finally agreed to the island of Saipan, a little-known US territory. Once he completed the deal, agents swooped in to arrest him, and he was soon transferred to stand trial in Delaware.[36]

During our discussions, 19 federal prosecutors and agents revealed to me that "you're going to be more willing to go after a cybercriminal with a lure" as compared to other transnational crimes.[37] One prosecutor commented that "anecdotally, lures are used more in cyber"[38] while another observed that lures are "a more important tool in cyber cases in my view than in many other cases."[39] Christopher Painter, who spent nearly 30 years in government including as a cybercrime prosecutor, Deputy Assistant Director of the Federal Bureau of Investigation's (FBI) Cyber Division, and the US's top cyber diplomat, shared these assessments: "There are a number of interesting examples that involve lure operations and then followed by extradition … There are likely more lure operations than there are extraditions with respect to this. There seems to me slightly more compelling reasons because of the way some countries treat cybercrime right now."[40] In fact, the US Secret Service has even created a center dedicated to determining which high value cybercriminals they can identify and lure to justice.[41]

---

[36] "Chinese Citizen Sentenced to 12 Years in Prison for Cyber-Theft and Piracy of Over $100 Million in Sensitive Software and Proprietary Data."
[37] Prosecutor 57, interview.
[38] Prosecutor 13, interview.
[39] Prosecutor 23, interview.
[40] Painter, interview. Painter served as Coordinator for Cyber Issues at the US Department of State (2011-2017), Senior Director for Cybersecurity at the White House National Security Council (2009-2011), Deputy Assistant Director of the FBI Cyber Division (2008-2009), and Principal Deputy Chief of USDOJ's Computer Crime and Intellectual Property Section (2000-2008).
[41] Federal Agent 11, interview, September 16, 2020.

However, the anecdotal nature of these observations immediately raises questions regarding their reliability. Primarily, the interviewees focused on comparing the usage of lure operations, rather than unilateral alternatives in general. Lure operations could very well be used more often in cybercrime. But, capture operations could be used more for other transnational crimes such that the usage of unilateral methods could overall be higher for those other offenses. Nevertheless, as will be discussed in Chapter 5, only terrorism prosecutions have employed capture operations in recent decades. And such a tool was only used in three cases since 2001, which mitigates this concern.

Additionally, there is no database that tracks the use of unilateral alternatives and could be consulted for corroboration. So, I first considered the credibility of the interviewees. Would they have an incentive to misrepresent these comparisons? If anything, they would have an incentive to downplay the use of unilateral alternatives given the extraordinary nature of these tools, their contested status under international law, and potential for diplomatic backlash. The fact that officials nevertheless acknowledged their use therefore lends credibility to their observations.

I also sought to interview officials who could provide the most holistic perspective on these comparisons. The vast majority of those I spoke with were based at the USDOJ headquarters and would have the broadest view of nationwide efforts. For instance, Lanny Breuer served as AAG for USDOJ's Criminal Division and oversaw all US federal criminal prosecutions from 2009 to 2013. He shared with me that "lures may be more likely in cybercrime because it has become much more prevalent, notorious, and serious now."[42] The once second-in-command of USDOJ, former Deputy Attorney General Rod

[42] Breuer, interview.

Rosenstein, reached the same conclusion since there are limited prospects for cooperation from host countries in cybercrime.[43]

These prosecutors were not only briefed on significant transnational crime prosecutions across the country but also set the nationwide strategy on bringing international fugitives to justice. Therefore, their insights offer the most complete view for comparing cybercrime to other forms of transnational crime.

Nevertheless, I recognized that such views from headquarters may not match the reality on the ground. Thus, I also spoke with prosecutors who worked in the most important US Attorney's Offices for prosecuting transnational crimes.[44] They offered similar insights, supporting the reliability of the reflections from headquarters.

Out of the 81 total interviews, six law enforcement officials disagreed. They did not believe that unilateral alternatives are used more often in cybercrime cases as compared to other transnational crimes. In response, I sought to understand the reasons for these beliefs. I discovered that each of these six individuals had either never been involved in a case involving a unilateral alternative or had a personal aversion to utilizing such methods. For example, one prosecutor only worked on cases involving cooperative host countries with which the US shares strong law enforcement relations and would have had no reason to turn to unilateralism.[45]

Likewise, one federal agent maintained that the FBI would not use a lure operation in a cybercrime case.[46] I then probed this claim with subsequent interviewees, and multiple prosecutors contradicted this by explaining they had personally worked with the FBI on lures in cyber cases. Based on these triangulation efforts, I concluded that these six

[43] Rosenstein, interview. Rosenstein is a career prosecutor who also served as US Attorney for the District of Maryland from 2005 to 2017.
[44] US Attorney's Offices are USDOJ's prosecutorial field offices, located in each of the 94 US federal districts.
[45] Prosecutor 30, interview.
[46] Hess, interview.

opinions are not representative of US efforts to secure custody over international cybercriminals.

The remaining law enforcement officials I interviewed simply did not comment on the relative frequency of unilateral alternatives. Some believed they lacked the data to confidently make such comparisons. Others believed that such comparisons were sensitive government information, which they could not publicly disclose.

Considering these findings, I now explore why there is a greater need for unilateralism in the form of lure operations in cybercrime cases. In Chapter 2, I hypothesized that cybercrime faces challenges related to the facts of the case, applicable laws, and political considerations. I now interrogate whether these predictions play out in practice.

4.2 Who Are You? The Persistent Hurdle of Attribution and Evidentiary Advantages of Lures

In this section, I explain how the difficulties of attribution present a major obstacle to securing custody over cybercriminals abroad. Pursuing countries may not know where the offender is located and thus which country to approach for assistance. They may also not have sufficient evidence to prevail on an extradition request. Yet, this obstacle can be overcome by a lure since the cybercriminal cannot credibly deny involvement after arriving and oftentimes carries evidence of his illicit conduct with him.

It wasn't me - some other dude did it! The SODDI defense is one of the oldest and most common criminal defense strategies. Yet, it poses a particular complication for cybercrime, especially for securing custody. Despite advancements in cyber forensics and investigations, it remains difficult to trace many cybercrimes to their source. Cybercriminals often take complex evasive measures, such as bouncing their attacks

through proxy servers in multiple countries or employing virtual private networks, to conceal their identities.

Several prosecutors lamented that it is a challenge "to pin down where cybercriminals are located."[47] If law enforcement does not know where the offender is residing, they also do not know which country they should approach with a request for extradition or informal cooperation through a quasi-extradition.

Even when law enforcement can narrow down the originating Internet Protocol address, they face the hurdle of linking that address to a specific person.[48] Milan Patel, a former FBI Special Agent and Chief Technology Officer of the FBI Cyber Division, explained to me, "By far, the hardest part is to put a human being behind the keyboard, the hands on the keyboard."[49]

It's challenging to not only identify the human perpetrator but also prove so beyond a reasonable doubt. The suspect can very easily claim some other dude did it. For example, the defendant can claim "the computer maybe a bot; it may have been hijacked. And so, attribution of conduct to an individual or individuals or actual persons is a huge challenge in the cyber realm."[50] The defendant can also claim that he has been a victim of identity theft. Or someone else might have had access to the computer and perhaps that other person was the one committing the crimes.[51]

Traditional law enforcement tools such as cooperating witnesses and undercover investigators may not even be able to overcome the attribution hurdle. Cybercriminals typically only communicate using nicknames. So, a cooperating witness or undercover

[47] Prosecutor 41, interview; Prosecutor 29, interview, August 13, 2019; Prosecutor 48, interview.
[48] Prosecutor 45, interview.
[49] Patel, interview.
[50] Prosecutor 17, interview.
[51] Prosecutor 39, interview.

agent posing as a co-conspirator may often still struggle to definitively establish the real-world identity of the target.

For other types of transnational crime, the target is usually identified at the start of the investigation. According to one prosecutor, with "more traditional white-collar crimes or gang crimes, I think pretty much you know who the players are. It's just connecting them to the crime whereas with cybercrime, usually the viability of a prosecution depended on whether you can even identify the perpetrator in the first place."[52]

This attribution challenge in cybercrime presents an immediate barrier to securing custody. One prosecutor detailed for me that "identity is going to be the central issue that the arresting or extraditing country is going to ask for. You can imagine the embarrassment if you get the wrong person."[53] So, if the pursuing country cannot prove attribution, the extradition request will fail.[54]

Likewise, the identification challenge may preclude waiting for the defendant to travel. Let's say that law enforcement suspects an individual and issues a Red Notice for his arrest. If he is caught in a third country, he will still need to be extradited from that country, and the pursuing country will still need to prove attribution.[55] Quasi-extradition does not solve this quandary either. Granted, this mechanism involves little to no legal process before the defendant is handed over. However, the pursuing country will still need to prove attribution in their domestic courts to secure a conviction.

Nevertheless, could these observations by US officials be overstated to justify the need for and use of unilateral tools? Well, the attribution challenge has been repeatedly corroborated by the existing literature on cybercrime. One study emphasized there is a common understanding that "attribution is one of the most intractable problems of [this]

[52] Prosecutor 58, interview.
[53] Prosecutor 57, interview.
[54] Prosecutor 44, interview.
[55] Federal Agent 7, interview, September 6, 2019.

emerging field, created by the underlying technical architecture and geography of the Internet."[56]

My conversations with foreign officials also independently confirmed the difficulties of attribution. For example, a German cybercrime prosecutor agreed that attribution is "pretty difficult, especially when it comes to more sophisticated attacks."[57] When I asked a Norwegian prosecutor about the problems in securing custody over international cybercriminals, the prosecutor immediately pointed to the attribution challenge and referenced the case of Mark Vartanyan.

This Russian cybercriminal was accused of developing and selling the Citadel virus. His trojan horse would enable users to steal personal information, such as banking details, from their victims. Once arrested in Norway on a US extradition request, Vartanyan presented expert witness testimony from a professor at the University of Oslo. The professor acknowledged that Citadel was linked to Vartanyan's Internet Protocol address but argued this was most likely because Vartanyan's computer had been infected with a virus. In other words, some other dude did it by compromising and then using Vartanyan's computer. As a result, the Norwegian district court denied extradition.[58]

While it is difficult to overstate the attribution challenge, it is also important to acknowledge that it does not impede all cybercrime cases. Cybercriminals may sloppily leave clues that link their nickname to their real-world identity. Some may even brazenly disclose their true names. For example, hacker Alexey Ivanov sent his resume and photograph to his victims as he attempted to extort employment opportunities.[59]

Traditional law enforcement tools, like undercover investigations, may prove effective in certain cases too. In the CRACK99 case, the undercover agent arranged Skype

[56] Rid and Buchanan, "Attributing Cyber Attacks," 5.
[57] German Prosecutor, interview.
[58] "Norway Refuses to Send Russian 'Hacker' to US."
[59] Cha, "A Tempting Offer for Russian Pair."

calls with Xiang Li, helping them to definitively establish his identity. In fact, once law enforcement penetrates a cybercriminal network, such as through social media, the difficulties of attribution may completely collapse since they may gain access to all the offenders' connections and evidence of the illicit conduct. However, this does not necessarily mean that cooperation in securing custody over the perpetrator will proceed smoothly. As we will see in the sections that follow, political obstacles may still create a need for unilateralism to bring cybercriminals to justice and stem the ongoing financial harms, even when attribution is known.

Plus, in the many cases where attribution remains a challenge, I learned that unilateralism in the form of a lure operation *can* overcome that hurdle. Throughout the lure, law enforcement is communicating with the perpetrator. Once the individual falls for the ruse and arrives, it is difficult for him to credibly deny involvement. One federal agent elaborated, "Lures are great because you get them but also defeat the SODDI defense, some other dude did it, in a cyber case. If I lure you and you're using your nick[name], what are you going to say? You can't say it was somebody else, right. You're here."[60] In fact, lure cases typically resolve through plea deals. Defendants recognize that proceeding to trial would be fruitless.[61]

Lures further resolve the attribution challenge by providing law enforcement with crucial evidence. Cybercriminals are "usually using a distributed workforce to carry out these schemes and they're very mobile. So [it's] not unusual to have them travel with their laptops."[62] Thus, once the offender is arrested on a lure, investigators can seize and search his devices for the evidence to knock the final nail in the attribution coffin.

[60] Federal Agent 11, interview, August 22, 2019.
[61] Federal Agent 11.
[62] Prosecutor 57, interview.

The anonymity of the internet not only creates a need for these lure operations but also increases their viability. "These guys communicate online with people they don't know," which creates an avenue to introduce an undercover investigator.[63] Jason Weinstein, who served as a Deputy Assistant Attorney General (DAAG) of USDOJ's Criminal Division and oversaw the Computer Crime and Intellectual Property Section (CCIPS), emphasized that cybercriminals are comfortable developing trust with others despite having never met in person. It is precisely this trust that law enforcement can exploit to lure perpetrators to their arrest.[64] Moreover, cybercriminals can be overconfident. They think that they have covered their tracks and obscured their identity. So, they may be more likely to risk traveling in response to the proper inducements.[65]

In 2010, Marriott International employees received a seemingly harmless email with an attachment. Little did they know, the attachment concealed malware that opened a backdoor into Marriott's networks. A Hungarian hacker, Attila Nemeth, exploited his newfound access to trawl Marriott's databases for proprietary emails and financial documents. His objective: blackmail. He soon contacted Marriott, threatening to release this confidential data unless he was given a job.[66]

Working with Marriott, US Secret Service agents launched an undercover investigation. They traced the attack to Nemeth but were not certain where he was located. Law enforcement knew that he had a Hungarian passport, but he may not have physically been in Hungary. Given the remote nature of his crimes, he could have been anywhere in Europe. Such movements within the Schengen Zone are not tracked, so agents could not

[63] Federal Agent 11, interview, August 22, 2019.
[64] Weinstein, interview, August 6, 2019. Weinstein previously served as the Assistant Chief of the Criminal Division of the US Attorney's Office for the District of Maryland as well as an AUSA in the District of Maryland and the Southern District of New York.
[65] Prosecutor 9, interview.
[66] "Hungarian Citizen Sentenced in Maryland to 30 Months in Prison for Hacking into Marriott Computers to Extort Employment from the Company."

simply have requested his passport data from Hungary either. Thus, they did not know which country to approach for extradition. Even if they issued a Red Notice, it would only be triggered if Nemeth flew. Additionally, federal agents needed further authentication he was indeed the individual behind the attacks to prove attribution.[67]

Consequently, law enforcement resorted to a lure operation. Since Nemeth was demanding a job, undercover agents decided to play along. To arrest him, they informed Nemeth that he would need to attend an in-person interview in either Europe or the US. He took the bait and chose the US.[68] During the interview, he admitted to the crimes and even demonstrated how he accessed Marriott's systems and where he was storing the stolen data in Hungary.[69] In that moment, the lure eliminated the attribution challenge. Nemeth not only arrived after communicating with the undercover agent but also confessed. As a result, he "didn't have much of a choice really" but to plead guilty.[70]

In addition to demonstrating the attribution challenge, this case mitigates against the alternative hypothesis posited at the beginning of the chapter. The US did not apply a lure operation here against a cybercriminal in a geopolitical rival. It applied this tool against a cybercriminal in a friendly state and North Atlantic Treaty Organization (NATO) ally, Hungary. This individual posed no national security threat nor was suspected of being a state actor. Indeed, if the US's use of lure operations were truly driven by geopolitics, it would not have risked alienating an ally against one of its key rivals simply to take down a lowly criminal. It thus appears the use of a lure here was motivated by a desire to bring an individual extorting a US company to justice rather than geopolitical objectives.

[67] Federal Agent 7, interview, March 17, 2021.
[68] Prosecutor 28, interview, August 9, 2019.
[69] "Hungarian Citizen Sentenced in Maryland to 30 Months in Prison for Hacking into Marriott Computers to Extort Employment from the Company."
[70] Prosecutor 28, interview, August 9, 2019.

Similar difficulties in attribution plagued the prosecution of Igor Klopov. This Russian cybercriminal was likewise not suspected of any ties to the state nor posed any national security threat. He was simply out to make a buck by culling the internet for the PII of wealthy Americans. Klopov's goal was to target their home equity lines of credit and create fake identification documents. He sent US-based co-conspirators into banks across the country to transfer funds from these lines of credit to other co-conspirators, who then passed them on to Klopov.[71] In total, this heist stole $1.5 million and attempted to steal a further $10.7 million.

The entire conspiracy relied on cyber-enabled means. So, one law enforcement official informed me that they struggled to definitively link the crimes to a real-world orchestrator.[72] This evidentiary challenge meant that extradition, quasi-extradition, and waiting for Klopov to travel were off the table.

Yet, law enforcement caught a lucky break. They arrested one of Klopov's US co-conspirators and assumed his identity. Investigators learned that Klopov had attempted to steal $7 million from a wealthy American to purchase gold bars. This now presented an opportunity for a lure operation to finally apprehend Klopov. Pretending to have obtained the gold, undercover investigators convinced him that he would need to travel to the US to obtain it. After entering New York via the Dominican Republic, Klopov was arrested.[73]

As in the Nemeth case, the lure operation overcame the attribution challenge in two ways. First, Klopov arrived after communicating with undercover investigators. In fact, he arrived wearing a certain type of Russian hat, the same type he had told undercover investigators that he would bring on the trip. Second, the lure provided critical evidence for a conviction. Klopov had previously told undercover investigators about the device he

[71] "News Release - August 16, 2007."
[72] Law Enforcement Official 3, interview, September 25, 2019.
[73] "News Release - August 16, 2007."

used for this scheme, which he had in his possession when he arrived. Additionally, the devices seized on Klopov contained some caches, messages, and photographs that undercover investigators had sent during the conspiracy.[74] Therefore, it was no surprise when Klopov was found guilty.

4.3 From the Comforts of Home: The Challenges of Securing Custody for a Remote Crime

In addition to the challenges of proving attribution, I find that securing custody is complicated by the remote nature of cybercrime. Offenders can operate from anywhere in the world and do not need to travel as part of the conspiracy. This means they can shelter indefinitely in uncooperative jurisdictions that will protect them from extradition.

A cybercriminal may just as easily be your teenaged neighbor hacking from his parent's basement as a member of an Eastern European organized crime group.[75] Unlike other transnational crimes which are based in the physical world, the remote nature of cybercrime allows perpetrators to be located anywhere on the planet. Accordingly, former Deputy Attorney General Rosenstein remarked to me that "cyber capacity breaks down international borders."[76]

As a result, perpetrators generally have no need to ever enter the victim country where they could be arrested.[77] Although some cybercrimes may require domestic partners to cash out or transfer the proceeds, prosecuting these individuals does not solve the problem either. They are often unwitting or very low-level members of the conspiracy. They are not the ones with the technical expertise but rather replaceable pawns. Thus, arresting them has little to no impact on ending the cybercrimes in progress or deterring would-be cybercriminals.

---

[74] Law Enforcement Official 3, interview, September 25, 2019.
[75] Rosenstein, interview.
[76] Rosenstein.
[77] D'Ambrosio, interview; Prosecutor 49, interview.

Given these limitations, law enforcement must increasingly rely on extradition and its alternatives to get their hands on the key perpetrators who are located abroad. Yet, cybercriminals are smart. Since they can operate from anywhere in the world, they choose to operate "in places where they feel like they can't be touched."[78]

In fact, out of the 81 law enforcement officials I spoke with, over 30 of them referred to cybercrime's remote nature as one of the central barriers in bringing cybercriminals to justice. For example, Michael DuBose, who was the CCIPS Chief from 2007 to 2011, elaborated to me that in cybercrime "you're more likely to have defendants or suspects operating from countries you don't have an extradition treaty with, you don't have law enforcement relations with."[79]

Law enforcement also cannot simply wait for cybercriminals to visit friendlier jurisdictions. Due to the remote nature of cybercrime, perpetrators typically have no business reason to travel. The crimes are almost entirely committed online. Plus, communications with co-conspirators are generally conducted through online forums, chat rooms, and other encrypted medium rather than face-to-face meetings.

Likewise, the prosecutors and agents I interviewed repeatedly emphasized that these criminals do not typically travel for pleasure on their own volition.[80] Secret Service Assistant Director D'Ambrosio lamented that "generally they're not going to fly to the US …. just on a whim. You would have to entice them to fly here."[81] The same applies to them visiting third countries that could have extradition agreements with the US or cooperate through a quasi-extradition.

Thus, law enforcement must smoke them out of hiding to arrest them. For this reason, former AUSA for the Southern District of New York James Pastore observed that

[78] Prosecutor 28, interview, August 9, 2019.
[79] DuBose, interview.
[80] Prosecutor 20, interview; Prosecutor 40, interview; Prosecutor 44, interview; Pastore, interview.
[81] D'Ambrosio, interview.

"lures may be more on the table" for cybercrime as compared to other transnational crimes.[82] DAAG Weinstein shared this assessment that the "actors are often clustered in countries where they are out of reach, so you frequently have to use a lure."[83] In other words, the remote nature of cybercrime, combined with the uncooperativeness of host countries, often leaves law enforcement with no option but a lure operation to ferret out perpetrators. But, why are these countries uncooperative?

4.4 The (Not So) Legal Barriers to Securing Custody

Originally, I predicted that certain countries would become cybercrime safe havens due to legal barriers. Dual criminality requirements and the political offense exception would block extradition, and jurisdictional conflicts would cause victim countries to turn to unilateral alternatives to preempt each other. However, the interview evidence was not consistent with these predictions.

Even though US officials might wish to overemphasize legal barriers to justify relying on unilateral tools, they repeatedly denied the presence of such obstacles. For example, AAG Breuer insisted, "The legal challenges are not the most difficult."[84]

In this section, I will show how dual criminality is no longer an obstacle since countries have adequately outlawed cybercrime. This is due, in large part, to the Budapest Convention, which has harmonized cybercrime legislation globally. Even in countries that do not yet have cybercrime laws, pursuing countries can charge the more basic underlying offense to succeed on an extradition request. Plus, the political offense argument generally does not hold water due to the inherently commercial nature of most cybercrimes. The US is also establishing international norms that delineate when state sponsored cyberattacks cross the line into criminal conduct and has only focused on prosecuting those cases.

---

[82] Pastore, interview.
[83] Weinstein, interview, August 6, 2019. As DAAG, Weinstein also oversaw the Organized Crime and Gang Section and the Human Rights and Special Prosecutions Section.
[84] Breuer, interview.

Finally, jurisdictional conflicts have been resolved cooperatively, oftentimes by countries talking to each other and determining who is best equipped to take the lead.

Granted, dual criminality requirements were once a hurdle for cross-border cybercrime prosecutions. Martha Stansell-Gamm, who was CCIPS Chief from 1999 to 2007, recollected to me, "I remember in the early years calling prosecutors overseas for help, and they would stand on one foot and then the other, saying, 'Gee, does our law cover this? Is it a forgery? Is it fraud? What the heck is it?'"[85] If overseas partners could not be convinced that their laws covered these crimes, they would then be unable to cooperate through extradition.

Nevertheless, I found that these types of conversations are largely a relic of the past. Over the last 20 years, most countries have adequately outlawed the core offenses in this area.[86] In fact, I learned that the Budapest Convention has been responsible for much of this progress. I had previously been skeptical of the Convention's international impact, especially given its regional origins at the CoE. Yet, prosecutors repeatedly praised this agreement for harmonizing cybercrime legislation between countries.

It is possible that US prosecutors promote an unduly rosy view of the Budapest Convention since the US supports the Convention's expansion as a matter of public policy. Indeed, the US seeks to convince countries to adopt the Budapest Convention rather than the alternate cybercrime treaty that has been put forth by its main rivals, China and Russia.

However, the statistics on the Convention's impact in harmonizing cybercrime legislation speak for themselves. 66 countries are party to the convention, another two have signed, and a further eight have been invited to accede.[87] It's also important to note that countries have followed through on their commitments and are generally compliant

[85] Stansell-Gamm, interview.
[86] Prosecutor 45, interview.
[87] "Chart of Signatures and Ratifications of Treaty 185."

with the Convention's provisions. I had doubted that compliance would occur due to the treaty's loopholes and lack of enforcement mechanism. Yet, prosecutors acknowledged that the treaty has established "more commonality on what is considered to be a computer crime essentially and that makes things easier obviously."[88]

Jan Kerkhofs, a Federal Magistrate in the Cyber Unit of the Belgian Federal Prosecutor's Office, similarly endorsed the effectiveness of the Budapest Convention. He noted that it has remained "time-resistant" in effectively addressing new cyber threats that have emerged since the Convention's adoption in 2001. Kerkhofs also welcomed the Second Additional Protocol to the Convention, which addresses evolving jurisdictional and trans-border issues, particularly related to electronic evidence gathering.[89]

Beyond its signatories, the Budapest Convention has generated a worldwide ripple effect. Many countries that are not parties have implemented its provisions, even borrowing its language word for word.[90] In recent years, 177 countries have undertaken reforms in their cybercrime and electronic evidence laws. This represents an impressive 92% of all countries. Of these countries, 152, or 79%, used the Budapest Convention as some guideline or source in developing their legislation.[91]

As well as addressing dual criminality concerns, the Budapest Convention includes procedural provisions to facilitate extradition. For example, a victim country may not have an extradition treaty with the host country. Nevertheless, if both countries are party to the Budapest Convention, Article 24 states that the Convention can serve as an extradition treaty between them for any of the covered offenses. Likewise, if the host country refuses to extradite its nationals, the Budapest Convention requires that country to domestically prosecute the offender, ensuring that justice is served.

---

[88] Prosecutor 29, interview, August 13, 2019; Prosecutor 42, interview.
[89] Kerkhofs, interview.
[90] Prosecutor 55, interview.
[91] Seger, "Results of Capacity Building and Impact on Legislation."

Furthermore, the Convention has created a ready-made community of trust and cooperation.[92] The parties frequently interact with each other at meetings of the Convention Committee, the approximately annual Octopus Conference on Cooperation Against Cybercrime, and other ad hoc events. This enables their representatives to develop relationships with peers from around the world, which I witnessed firsthand at the 2019 Octopus Conference. Countries are then more likely to cooperate in investigations or extradition requests based on these personal connections. Prosecutors reported that there would be "no reason to attempt a lure from any member state of Budapest" based on any legal inadequacies of that convention.[93]

The Budapest Convention has still faced some resistance in certain parts of the world. The treaty was originally drafted by the CoE, so it is viewed by some countries as an exclusive Western club.[94] One prosecutor candidly acknowledged to me:

> It was drafted initially, ratified by a bunch of mostly white people in Europe and a few white people in the Western Hemisphere. It's considered a tool of the West … That's why it's just hard to get a lot of traction in Asia. We preach the benefits of the Budapest Convention to the countries that we're working with … [but] I don't think you're going to see many more or any ASEAN countries accede to the convention.[95]

Unfortunately, many of these countries are the same few that have not yet enacted adequate cybercrime legislation. As a result, dual criminality could block extradition from those countries. However, this shortcoming has not driven pursuing countries to unilateral alternatives as I expected. Although US officials might have an incentive to play up this obstacle, another prosecutor clarified that "the most significant cybercrime players aren't in those places. They're not in Africa. They're not in some parts of Asia where you're more likely to come across a country that has little or no legislation on cybercrime or a

[92] Prosecutor 55, interview.
[93] Prosecutor 29, interview, August 13, 2019.
[94] Prosecutor 44, interview.
[95] Prosecutor 58, interview.

police agency that has no experience in it."[96] Hence, these defendants simply are not important enough to justify unilaterally deviating from the extradition system.

Rather, I learned that prosecutors can often easily resolve this challenge by charging the underlying offense, such as fraud. These more basic crimes would easily be covered by both countries' laws, preventing any dual criminality challenge. One prosecutor expressed that "in terms of dual criminality, I have found that if you go back to first principles and put aside the overlay of cybercrime and the malware and other tools; go back and look at what sort of crime you're really dealing with; break it down to first principles like trespassing, fraud, money laundering; and structure your case around those principles, the dual criminality problem is not as significant."[97]

Based on these charging techniques and legal improvements abroad, prosecutors asserted that there are no longer dual criminality concerns in cybercrime.[98] In fact, one prosecutor observed that no extradition has been blocked on dual criminality grounds in recent years.[99]

I also predicted that extradition in cybercrime would be hindered by the political offense exception. AAG McCord summarized these concerns that "when you're talking about accusing actual government entities of [cyber]crime, then you automatically have not only diplomatic ramifications but the potential accusation of this is political. This is spying. This is what countries do and you don't typically indict people, countries for spying and don't we [the US] do the same thing."[100]

This legal obstacle also relates to the alternative hypothesis raised at the start of this chapter. Let's assume the US is using criminal prosecutions to undermine the cyber

[96] Prosecutor 29, interview, August 13, 2019.
[97] Prosecutor 57, interview.
[98] Prosecutor 14, interview; Prosecutor 33, interview; Prosecutor 39, interview; Prosecutor 40, interview; Prosecutor 18, interview.
[99] Prosecutor 18, interview.
[100] McCord, interview, August 14, 2019.

capacity of rival powers and take out these countries' cyber talent. If a state sponsored cybercriminal were arrested while travelling in a third country, he could claim that his conduct was merely espionage or another political offense. He could argue that the US was illicitly seeking to criminalize normal national security activity. The arresting country may therefore deny extradition, prompting the US to pursue unilateral action.

However, prosecutors reported that the "political offense [argument] doesn't usually gain traction."[101] Why is this? Are US prosecutors cleverly choosing which charges to include in their indictments in order to create a façade for prosecuting political crimes and fool arresting countries? Or, have their efforts indeed focused on truly criminal conduct?

To answer these questions, I looked to the first US indictment against state actors for cybercrimes. In May 2014, USDOJ charged five military officers of the Third Department of the Chinese People's Liberation Army (PLA) with computer hacking and economic espionage. On its surface, this case raises legitimate concerns that it was politically motivated and influenced by the ongoing cyber competition between the US and China. AAG McCord acknowledged these propositions but clarified:

> It was not classically governments spying on each other for strategic, military, or other reasons. It was to steal commercial information, trade secrets, business strategies, litigation strategies from major American corporations in certain sectors and to use those for the benefit of Chinese state-owned enterprises. So, the red line that was crossed was using cyber enabled means to obtain essentially a commercial advantage for your own companies, which is different than the normal type of tradecraft that most countries with the capacity to do so engage in.[102]

The five military officers charged have never been apprehended, and this case has never resulted in an extradition request. Yet, it set a precedent for the types of state sponsored cybercrime prosecutions that the US has pursued and have proceeded through extraditions.

---

[101] Prosecutor 44, interview.
[102] McCord, interview, August 6, 2020.

The following month, Canadian authorities arrested a Chinese businessman, named Su Bin, on a US extradition request. From 2008 to 2014, he had conspired with hackers from the PLA Air Force to break into US computer networks and steal military technical data. One such piece of data was the design plans for the Boeing C-17 strategic transport aircraft. This theft enabled China to build their own version of the C-17 in a third of the time it had taken the US. Su Bin directed the hackers as to which individuals, companies, and technologies they should target. The hackers then sent Su Bin the directory file listings so that he could instruct them which files and folders to steal. Su Bin subsequently translated the information into Chinese and issued reports to the Second Department, General Staff Headquarters of the PLA.[103]

When he was arrested in Canada, Su Bin could have argued that his crimes were political offenses. After all, this case toes the line of espionage much closer than the previous PLA indictment. Instead of benefitting Chinese corporations, the information Su Bin helped collect benefitted the Chinese Air Force. However, AAG McCord emphasized to me "[The data was] stolen from a private company. It wasn't stolen from a department … Don't countries spy on each other? Yes, they do, but this is [different] when you start involving private corporations and for-profit companies."[104] McCord analogized the case to an insider stealing physical files from a US corporation to send back to their home country's government. There would be "no question that that's unlawful and worthy of prosecution and not a purely political offense."[105]

Plus, Su Bin was engaging in the conduct for personal financial gain and sought to profit from the data he was selling.[106] For these reasons, the commercial nature of his

[103] "Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison."
[104] McCord, interview, August 6, 2020.
[105] McCord.
[106] "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information."

actions destroyed any claims that they were political offenses. Without this as a viable defense, Su Bin simply waived extradition. By actively pursuing extraditions from cooperative third countries in cases like this, the US has sought to repeatedly demonstrate that they are not political offenses and establish precedent that extradition can succeed.[107]

Evidently, US prosecutors have drawn certain distinctions between the commercial nature of the cybercrimes they are prosecuting and legitimate national security activity by states. But, is this line-drawing just a further effort to pretty up its use of law enforcement tools to advance geopolitical objectives?

As a matter of fact, the US has been joined by other nations in adopting these international norms and drawing a red line that the theft of trade secrets from corporations is beyond the acceptable bounds. Even one of the most prominent targets of US prosecutorial efforts here, China, agreed to norms against the state sponsored theft of IP to benefit companies or the commercial sector.[108] Two months later, the same norm was adopted by the Group of 20 (G20).

Based on these norms, AAG McCord explained, "the argument of a political offense [is] less susceptible to prevailing where the community of nations has agreed that this type of government sponsored cyberattacks for economic gain is not a political offense. It's a criminal offense."[109] This international agreement also undermines the alternative hypothesis that the US is illicitly targeting cyber actors in rival powers solely for political or national security reasons.

In addition to the political offense and dual criminality obstacles, I hypothesized that cybercrime cases would face a third legal barrier: their remote, global nature would generate jurisdictional conflicts. As multiple countries are victimized, each would jockey

[107] Prosecutor 4, interview, August 6, 2019.
[108] "Fact Sheet: President Xi Jinping's State Visit to the United States."
[109] McCord, interview, August 6, 2020.

to prosecute. With no clear legal criteria for prioritizing these jurisdictional claims, I posited that countries would resort to lure operations to preempt each other.

Nevertheless, my conversations with US prosecutors and agents revealed that this type of jurisdictional conflict has not materialized.[110] In the early 2000s, other countries lacked the interest or capacity to prosecute cybercrimes. Chief Stansell-Gamm recalled, "I actually mediated more fights between jurisdictions in the US than I did among countries. I would have been pretty excited to see other countries aggressively prosecute computer crime."[111]

In certain instances, other victim countries did not have adequate cybercrime laws in place. In other instances, their law enforcement lacked the technical know-how to investigate and prosecute such cases. Often, it was a combination of both. Therefore, these countries would not bring competing cases, and there would be no need for the US to use a unilateral alternative to win a jurisdictional battle.

Even as other countries have improved their laws and investigative capacity, they have typically deferred to the US. They recognize that the US remains the country best equipped to successfully investigate and prosecute cybercriminals.[112] As one prosecutor explained to me, "the reality is that the US is kind of the big boy on the block, and we probably have the most sophisticated mechanisms for dealing with this, particularly if we're going to get the body and we're going to actually prosecute an individual."[113]

There are still certain cases where other victim countries wish to prosecute domestically. However, these overlapping jurisdictional claims have always been resolved cooperatively, not unilaterally. Although it has not happened that frequently, Chris Painter

[110] Painter, interview; Prosecutor 27, interview; Prosecutor 35, interview; Prosecutor 40, interview; Prosecutor 42, interview; Pastore, interview; Prosecutor 55, interview.
[111] Stansell-Gamm, interview.
[112] Prosecutor 14, interview.
[113] Prosecutor 17, interview.

explained that countries may work together to prosecute the case serially. In other words, the defendant could be prosecuted in one country, serve his sentence, and then be extradited to stand trial in the next country. This approach vindicates each jurisdiction's desire for justice.[114]

In most cases, the prosecutors in each victim country collaboratively decide the best location for the cybercriminal to stand trial. According to AAG McCord, they weigh "the strength of the evidence under our various laws and who's likely to get a conviction … [and] where do the equities [lie] in terms of the victims and who suffered the most injury."[115] Prosecutors also contemplate the sentence that the defendant could receive in each jurisdiction and its appropriateness.[116]

Indeed, law enforcement officials shared with me that meaningful prosecution in the host country is a satisfactory outcome. The desire for justice does not always demand that the defendant be prosecuted in each pursuing country's courts. In fact, Chief DuBose revealed that at times, prosecution in the host country was preferable:

> In my experience, if they wanted to prosecute, unless we thought it was going to be a sham prosecution, we were more than happy to have them do it. It was faster. I think one of our goals was to support prosecutions in other countries to make this something that country would want to do and have success doing because success breeds more success and the better the case that we could develop with them and … frankly the more success that law enforcement agency had with the prosecution, the more likely they would be to assist on another.[117]

There may be incentives here for US prosecutors to present an overly optimistic view of the US's cooperativeness and willingness to defer to foreign jurisdictions. Yet, this approach has clearly manifested in multiple global cyber takedowns where each country arrested and prosecuted the offenders in their jurisdiction. Plus, given the scale of cybercrime, these insights make sense. The US cannot possibly prosecute every

[114] Painter, interview.
[115] McCord, interview, August 14, 2019.
[116] Prosecutor 14, interview.
[117] DuBose, interview.

cybercrime that passes through its borders. It simply lacks the resources for such a behemoth task. So, if another country is willing to assume the burden and meaningfully prosecute, passing the buck is squarely within the US's interests.

Considering the above findings, the only meaningful legal barrier that may remain is the lack of an extradition treaty with the host country. However, this barrier is not unique to cybercrime. It is a constant that would afflict all transnational crimes emanating from the host country in question. And, it does not necessarily create a need for unilateral alternatives. Countries can negotiate ad hoc agreements to hand over a cybercriminal in a specific case. The victim and host countries could also agree to a quasi-extradition, which does not require an extradition treaty, as occurred in the Seleznev case. An informal handover may be easier than an extradition since the victim country would not need to satisfy any evidentiary or legal requirements.

Even if the host country's laws prevent them from pursuing these other methods of cooperation, there is still a route to justice. The host country could prosecute the cybercriminal in their domestic courts. As I learned, host countries have largely outlawed cybercrimes, providing them with the domestic statutes in place to prosecute these offenses. Even if such laws do not exist in the host country, they can rely on charging the more basic underlying crime, such as fraud. Therefore, the lack of an extradition treaty does not, on its own, necessitate unilateralism. Other avenues of cooperation remain available. If a host country elects not to pursue these avenues, the failure of cooperation cannot be attributed to legal barriers.

4.5 The Lack of Political Will

If the need for unilateral alternatives in cybercrime does not stem from legal challenges, where does it originate? Why are pursuing countries still using such tools when we have robust legal instruments, such as the Budapest Convention? As AAG

Breuer declared, "it is mostly a political challenge."[118] In this section, I explore specifically how politics impedes cooperation in cybercrime. I learned that oftentimes countries lack the political will to assist in bringing these perpetrators to justice. These crimes generally do not cause domestic harms, so local officials can win a political victory by standing up to the pursuing country and denying cooperation. The stakes seem lower in cybercrime since it is a nonviolent offense. Plus, there can be greater public sympathy for these perpetrators.

Assisting on an extradition request may demand substantial resources from the host country. They not only have to execute warrants but also defend them in court. Since cybercriminals are smart enough to not target their fellow citizens, host countries may not see these cases as worth their while.[119] However, this same issue could arise for extradition requests related to other transnational crimes. It is not uncommon for a victim country to request the extradition of a perpetrator whose conduct has not touched the host country.

One prosecutor provided further explanation: "there's also a little bit of a nationalistic aspect to this and maybe a nationalistic pride that a hacker in our country, often a young person, had the skill to defeat the security of a major US corporation or government entity. And so, there's a little bit of a hometown aspect to it that I don't think applies to local murderers."[120] This challenge manifested in the Gary McKinnon case. Hugo Keith, the Queen's Counsel who represented UK Home Secretary Theresa May in the McKinnon extradition proceedings, reflected to me, "There was a latent sense, I think, among some people of, well, good for you. You've shown the world the [US] Defense Department system is not immune to hacking and is vulnerable."[121]

---

[118] Breuer, interview.
[119] Federal Agent 7, interview, September 6, 2019; Prosecutor 18, interview.
[120] Prosecutor 23, interview.
[121] Keith, interview.

More broadly, local politicians can score political points with their citizens by standing up to the pursuing country and denying cooperation. This also applied in the McKinnon case where "there was outrage in the UK, and there were songs written about him and all of that to protect him from the evil US who wanted to bring him to justice."[122] While US officials may have a biased perspective here and wish to blame the outcome on politics, UK officials involved in the case have corroborated this account. The UK Director for Public Prosecutions noted that when Theresa May blocked extradition, "'none of the reasons for the original decision in 2002 that the appropriate place for Mr. McKinnon to be tried was the United States have altered.'"[123]

The former Home Secretary, Alan Johnson, also explained that McKinnon's appeals had been rejected by the courts. But, it became politically advantageous for Theresa May to block extradition, so she "made the decision 'in her party's best interest; it is not in the best interests of the country.'"[124] Indeed, there were six parliamentary by-elections coming up within weeks of May's decision, including one where a seat from her party was up for grabs. Still, this political will barrier is not necessarily unique to cybercrime. Local politicians can benefit from denying cooperation for any offense.

Nevertheless, I discovered that characteristics of cybercrime make it easier for local officials to say no. It is usually a nonviolent offense and thus presents a less clear threat than other crimes. In our conversation, AAG Breuer reflected that "cybercrime is so amorphous. It doesn't seem as real as other types of crime, so it's hard to get parties invested enough in it."[125]

And this is not just the perspective of US officials. A senior English barrister agreed, particularly with respect to the Lauri Love case. The barrister explained to me that

[122] Prosecutor 2, interview.
[123] Williams, "Computer Hacker Gary McKinnon Will Face No Further Action Says CPS."
[124] Travis and Bowcott, "Gary McKinnon Will Not Be Extradited to US, Theresa May Announces."
[125] Breuer, interview.

the crime was considered less significant since "the people affected were affected indirectly … There's never any doubt that terrorism is always serious. People trafficking is always serious. Drugs, all the rest of it. But there just doesn't seem the same value to be ascribed to the impact of cybercrime."[126]

As another example, Kim Dotcom, a New Zealand resident, stands accused of running a massive online piracy conspiracy through the file sharing platform, Megaupload. The site distributed copyright infringing copies of movies (often before their release), music, television programs, eBooks, and other software. The scheme netted $175 million in profits and caused over half a billion dollars in harm to the copyright holders. The US requested Dotcom's extradition from NZ in 2012. Yet, the case remains unresolved. One US prosecutor revealed that it has been hard to garner support for extradition in NZ since the charged conduct "doesn't resonate with people."[127]

The harm of not cooperating on a cybercrime case just seems minor compared to another type of transnational crime. So, local officials can afford to take the political win instead of assisting. Some countries even adopt the perspective that is the victims' fault for being foolish enough to fall for certain cyber frauds.[128]

Cooperation is further impeded by disagreements between countries as to what behavior crosses the line between permissible conduct and illegal acts. Even when countries have joined the Budapest Convention, interpretations of its provisions may differ. One prosecutor noted, "even though I'm sure there are laws against [cybercrime], it's just not considered criminal in the same way … Hacking laws exist in almost every country. But if you're asking [host countries] to analyze whether the hack is a crime, it's a harder thing."[129]

---

[126] Senior English Barrister 1, interview.
[127] Prosecutor 44, interview.
[128] Prosecutor 6, interview.
[129] Prosecutor 28, interview, August 9, 2019.

For example, certain host countries are more willing to tolerate recklessness or foolishness on part of their citizens in hacking computer systems. This is particularly true if there is no clear economic gain. As a result, one prosecutor explained to me that this lack of consensus "can be a barrier because other countries are not going to be invested in supporting extradition for conduct they don't see as criminal."[130] As AUSA Pastore observed, these types of clashes are more common for cybercrime. In other areas, there is simply less room for disagreement as to what is a crime. For instance, he remarked, "We all know drug trafficking is a crime."[131]

The profile of cybercriminals provides yet another reason why host countries may lack the political will to cooperate. It is far easier to humanize these defendants. It is far easier to think of them as your neighbor's kid rather than a violent terrorist or drug trafficker. For instance, "the common perception is that the middle class accounts for a higher proportion of offenders than it does in other crime types."[132]

Additionally, there is a widespread belief that cybercriminals experience a higher incidence of autism spectrum disorders, specifically Asperger's syndrome.[133] In fact, one prosecutor I spoke with observed that the solitary nature of these crimes may lend itself to attracting individuals with such conditions.[134] A senior English barrister concurred that "a lot of people who have Asperger's get into computers … [so] it's perhaps a predictable feature of these cases."[135] It thus becomes easier to sympathize with these defendants and write off their criminal conduct as partly owing to their psychology.

For example, the UK was moved to deny extradition for McKinnon and Love over concerns for their wellbeing as individuals with Asperger's syndrome. In her statement to

[130] Prosecutor 2, interview.
[131] Pastore, interview.
[132] Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*, 15.
[133] Lusthaus, 12.
[134] Prosecutor 39, interview.
[135] Senior English Barrister 1, interview.

the UK House of Commons, Theresa May explained, "there is also no doubt that [McKinnon] is seriously ill. He has Asperger's syndrome and suffers from depressive illness … I have concluded that Mr. McKinnon's extradition would give rise to such a high risk of him ending his life that a decision to extradite would be incompatible with Mr. McKinnon's human rights."[136] The High Court of England and Wales reached a similar conclusion for Love.

While the condition of the US prison system partly influenced these decisions, that was not the sole determining factor. In the Love case, a senior English barrister recalled that there was "certainly less a concern about the US prison system. All prison systems are struggling at the minute … and anyone who looks closely at the UK's own prison system would form the same view."[137] Likewise, former UK Home Secretary Johnson explained that the US had offered to let McKinnon carry out his prison sentence in the UK, eliminating that concern.[138]

Plus, merely two weeks after May blocked McKinnon's extradition, the UK extradited Syed Talha Ahsan, who also suffered from Asperger's and depression, to the US. Indeed, "'a psychiatrist had predicted a high risk of serious depression leading to suicide if [Ahsan] were to be extradited and placed in solitary confinement for a long period.'"[139] However, Ahsan was accused of terrorism offenses: running jihadi websites and raising funds for the Taliban.[140]

Given the near identical mental health concerns, these contrasting decisions demonstrate the outcome was less about the US prison system and more about the type of crime. McKinnon's cybercrimes generated public sympathy and were non-violent, neither

[136] May, "Theresa May Statement on Gary McKinnon Extradition."
[137] Senior English Barrister 1, interview.
[138] Travis and Bowcott, "Gary McKinnon Will Not Be Extradited to US, Theresa May Announces."
[139] Doyle, "McKinnon and Ahsan: A Tale of Two Extraditions."
[140] Doyle.

of which described Ahsan's terrorist activity. Therefore, the former had greater political implications than the latter. Indeed, a senior English barrister acknowledged to me, "If McKinnon had died in an American prison suffering from autism and severe depression, which he had, or committed suicide, the Home Secretary who extradited him would undoubtedly suffer politically. There's no doubt about it. If it was [a terrorist], no one would care."[141]

Due to all the above factors, prosecutors reported that "it was hard to get countries interested in" cybercrime.[142] Thus, these host countries would not cooperate via extradition or quasi-extradition, which would leave law enforcement with unilateral alternatives.

Nevertheless, have these challenges played out in any cases where the US has applied unilateral tools? I found that they posed the major obstacle to securing custody in the case described at the beginning of this chapter. Two Romanian cybercriminals, Iulian Dolan and Cezar Butu, participated in a scheme to hack into the point-of-sale terminals of hundreds of US retailers. They installed keystroke loggers, capturing the payment card information passing through these machines. Their co-conspirators exploited this pilfered data to rack up unauthorized charges or transfer funds to their account. By the time the two-year conspiracy came to an end in 2011, they had compromised over 146,000 payment cards and caused more than $10 million in losses.[143]

On the surface, the case appears to be a slam dunk for extradition. There is clear criminal conduct attributed to Dolan and Butu. The US has an extradition treaty with Romania. What could go wrong? When Romania was approached by US law enforcement, they saw it as an opportunity to score political points. One US federal agent recalled to me

[141] Senior English Barrister 2, interview.
[142] Law Enforcement Official 1, interview; Prosecutor 20, interview.
[143] "Two Romanian Nationals Plead Guilty to Participating in Multimillion Dollar Scheme to Remotely Hack into and Steal Payment Card Data from Hundreds of US Merchants' Computers."

that the then Prosecutor General of Romania, Laura Codruța Kövesi, declared, "'We will extradite a Romanian when you extradite a US citizen to Romania.'" The agent elaborated, "It [was] more of a public opinion thing. Like we're not gonna be bullied around by the big [US] federal government."[144] Since these cybercrimes were not viewed as serious offenses in Romania, it was easier to take a stand and deny cooperation.

However, given that there is an extradition treaty in place, the principle of extradite or prosecute would oblige Romania to domestically prosecute the offenders. Yet, since these cybercrimes completely avoided Romanian victims, Romania had no interest in prosecuting the case. Plus, Dolan and Butu would have likely escaped with no more than a one-year prison sentence.[145] Afterwards, they could have easily returned to their old ways, hacking US businesses. Thus, prosecution in Romania would have hardly vindicated US interests or served as a deterrent.

Quasi-extradition was not an option either since Dolan and Butu were Romanian citizens. Therefore, Romania could not simply deport or expel them. US law enforcement also could not wait for them to travel to a more cooperative country. The tracking of their movement was too delayed. Federal agents often would not find out Dolan and Butu were in another country until they posted on social media. At that point, it would have been too late to catch them.[146] Therefore, law enforcement turned to a lure as a last resort.

For Butu, law enforcement pretended to be a beautiful blonde woman whom he had met on vacation. Gaining a knack for female impersonation, the undercover agent adopted a similar approach with Dolan and played off his prolific online gambling. Posing as a female casino employee, the agent offered Dolan a free trip to a US casino, which he

[144] Federal Agent 11, interview, August 22, 2019.
[145] Federal Agent 11, interview, February 18, 2020.
[146] Federal Agent 11, interview, August 22, 2019.

eventually accepted. But instead of being greeted by a driver to the casino after he landed at Boston Logan Airport, Dolan was greeted by federal agents.[147]

Given the nonpublic nature of internal deliberations as well as conversations between US and foreign law enforcement officials, it is impossible to know whether the narrative shared by US officials is complete and accurate. However, two factors lend credibility to these findings. First, the alleged lack of political will in the Dolan and Butu case is consistent with the general concerns that cybercrime prosecutors independently raised. Second, I conducted two interviews regarding this case with the federal agent, who provided an identical narrative despite over four months passing between our conversations. The agent did not waver from or contradict any previous statements.

The Dolan and Butu case and the revelations in the section also mitigate against the alternative hypothesis. The political challenges of bringing cybercriminals to justice are not only experienced with rival powers. Indeed, the US even struggled to secure custody over two high profile cybercriminals from its closest and longest standing ally, the UK. Plus, it again applied a unilateral alternative against a NATO ally in the Dolan and Butu case. These perpetrators were merely profit-oriented con men who had no connection to the state or involvement in intelligence activities. This further suggests that the US is not simply applying lures to accomplish geopolitical objectives. Rather, it appears to be pursuing legitimate law enforcement goals to end clearly criminal conduct.

4.6 The Specter of State Sponsorship

In this section, I explore another way in which politics impedes international cooperation in cybercrime cases: state sponsorship. Specifically, certain states value the skills of cybercriminals and wish to coopt them to accomplish state objectives. So, these countries seek to protect cybercriminals from prosecution abroad. State sponsors also seek

[147] Krebs, "Alleged Romanian Subway Hackers Were Lured to US."

to undermine the chances of these fugitives being brought to justice if they travel abroad by undermining international consensus on cybercrime and interfering in the extradition process.

Given the inescapable interplay of geopolitics here, there is a concern that the US is simply luring cybercrimes to undermine the cyber talent of its rivals. I further engage with that alternative hypothesis in this section. I ultimately determine that the evidence mitigates against it. The US has solely focused on prosecuting cyberattacks that cross internationally agreed norms and has been joined by other countries in denouncing such conduct. I also learned the US national security apparatus has preferred to track and monitor such cyber threats. This helps explain why all known lure operations have only involved private cybercriminals rather than state actors.

In 2014, the internet giant Yahoo suffered the largest reported data breach to date. Hackers had gained access to the sensitive data of 500 million users, including names, email addresses, telephone numbers, birthdates, and encrypted passwords.[148] However, the perpetrators were no ordinary cybercriminals. A 2017 USDOJ indictment revealed that the hack was a collaboration between two cybercriminals, Aleksey Belan and Karim Baratov, and two Russian Federal Security Service (FSB) officers.

The Yahoo case suggests a disconcerting evolution of cybercrime into a blended threat between profit-motivated crimes and state sponsored activities. As one prosecutor described to me, "you have cyber criminals that may be operating on their own for their own financial gain, but digging deeper, they're actually funded or supported by the government."[149]

[148] Condliffe, "A History of Yahoo Hacks."
[149] Prosecutor 2, interview.

This is precisely what occurred in the Yahoo hack. Belan exploited the breach to steal gift card and credit card numbers, deploy 30 million accounts in a massive online spam campaign, and redirect Yahoo's search engine traffic for a commission. All these activities solely served to line his pockets. Simultaneously, he gained access to at least 6,500 Yahoo email accounts without permission. The accounts were not selected at random but rather were targets of interest to Russian intelligence. They included Russian journalists, Russian and US government officials, and employees of a leading Russian cybersecurity company.

In exchange for this espionage work, the FSB officers protected Belan by feeding him sensitive law enforcement information to escape detection by US authorities. According to AAG McCord, this conduct was "beyond the pale" since the FSB officers belonged to the same unit that was the FBI point of contact in Moscow on cybercrime.[150]

State sponsorship evidently exists on a spectrum. It ranges from state actors, such as military and intelligence officers, committing officially sanctioned cybercrimes to state actors moonlighting for personal enrichment to private cybercriminals assisting the state to private cybercriminals receiving the tacit protection of their government. Certain countries recognize that cybercrime can provide benefits like illicit proceeds and stolen IP without harmful domestic impacts.[151] As a result, they support cybercrime as a matter of policy.

Based on this shrewd calculus, AUSA Pastore observed that state sponsorship "may have a meaningful impact in distinguishing cybercrime from other transnational crimes since states may view hackers as an asset but not necessarily the fraudsters … In drug trafficking, you can see some close connection between drug dealers and the state, but it's not to the same extent."[152] Host countries understand that providing safe haven to

[150] "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."
[151] Prosecutor 21, interview.
[152] Pastore, interview.

cybercriminals can be a bargaining chip to coopt these offenders into pursuing state objectives in the future. Indeed, Marc van der Ham, a Senior Legal Advisor at the High Tech Crime Unit of the National Office of the Dutch Public Prosecution Service and External PhD Candidate at Leiden University, explained to me that "some countries may provide safe haven to skilled criminals for geopolitical reasons and, as a reward, allow criminal operations to be launched from their territory."[153]

Consequently, state sponsors will not hand over their cybercriminals either through a formal extradition or quasi-extradition. A German prosecutor elaborated to me that "those countries do not play a role in our investigations because we know they won't respond to any form of requests."[154]

State sponsors may at times appear amenable to cooperation, but I learned that pursuing countries should not be fooled. These overtures conceal a hidden objective: to trick pursuing countries into revealing their intelligence. Chris Painter reflected that "you're locked in this interesting problem where you can go to that government that was responsible … and they'll say, 'Well, give us all the information you have on this' and they use that information to improve their TTPs [tactics, techniques and procedures] and to find out … what you have on them."[155] In the end, the cybercriminal will never be handed over or will receive a mere slap on the wrist from the state sponsor's courts. But, the state sponsor will have learned how to avoid detection for future cybercrimes.

State sponsors also seek to protect their cybercriminals by undermining international consensus on cybercrime. China and Russia have championed a new United Nations cybercrime treaty to replace the Budapest Convention. They claim the goal is to develop a truly universal agreement on cybercrime. However, the prosecutors I spoke with

[153] van der Ham, interview.
[154] German Prosecutor, interview.
[155] Painter, interview.

believe that it is really designed to splinter the international community, "reshape the cyber landscape and further protect cybercriminals."[156] As Chris Painter observed, "It's a waste of time, will take forever, and be a lower level and not likely to stop these issues."[157] For instance, one of Russia's principal objections is that the Budapest Convention infringes norms of state sovereignty and non-interference.[158] A new treaty that defers more to such principles would provide host countries with greater pretense to deny assistance and shield their cybercriminals.

Nevertheless, I did not need to simply accept the word of US officials here. A German prosecutor shared the view that the new treaty "will be a race to the bottom, that's for sure, and probably won't have the goal of giving the broadest possible means for investigators and prosecutors to cope with this transnational crime."[159] Marc van der Ham elaborated that the "Dutch government is likely very skeptical of the UN treaty and its political motivations. It's not compatible with the multi-stakeholder model."[160]

Plus, I witnessed firsthand Russia's efforts to undermine consensus at the 2019 Octopus Conference. During the opening session, a Russia official requested to make an unscheduled presentation. His objective: to encourage states to support the proposed UN convention and abandon focus on the Budapest Convention. While the Russian representative highlighted the need for a global cybercrime treaty, he provided no explanation why the Budapest Convention was inadequate. Nor did he offer any reasons why the international community should not simply focus on convincing more countries to join the Budapest Convention.[161]

---

[156] Prosecutor 52, interview.
[157] Painter, interview.
[158] Hakmeh and Peters, "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet."
[159] German Prosecutor, interview.
[160] van der Ham, interview.
[161] Chernukhin, "Countering the Use of Information and Communication Technologies for Criminal Purposes."

In response to this intervention, multiple participants from around the world stressed how negotiations on a UN treaty merely serve to thwart consensus and protect cybercriminals. Not a single attendee from the 116 countries present expressed support for Russia's proposals. Alexander Seger, Head of the CoE Cybercrime Division and Executive Secretary of the Cybercrime Convention Committee, raised concerns that the efforts to pass a new UN treaty risk creating greater division and polarization on cybercrime matters.[162] Likewise, Claudio Peguero, Advisor to the Director General of Police in Cyber Matters for the National Police of the Dominican Republic, contended that "today, we have victims who demand a response from the criminal justice system …While we negotiate new instruments, we are generating impunity … because the problem exists today."[163] In other words, countries may delay essential actions on improving their cybercrime laws as they await the possible creation of a new UN treaty, allowing perpetrators to escape justice. As the international community becomes more fractured on cybercrime, it also becomes less likely for third countries to arrest and hand over foreign cybercriminals who visit their country.

State sponsors have even gone a step further when their cybercriminals have been arrested in third countries. They have interfered in the extradition process to snatch back their citizens and provide safe haven.

Secret Service Assistant Director D'Ambrosio recalled the case of Farkhad Rauf Ogly Manokhin. This Russian national belonged to a cybercriminal network that used malware to steal victims' banking information and ultimately caused $100 million in losses.[164] In 2017, Manokhin vacationed to Sri Lanka with his family, which abruptly ended with him in handcuffs. Local authorities had arrested him at the request of US law

[162] Seger, "Opening Session."
[163] Peguero, "Opening Session." Translation by author.
[164] D'Ambrosio, interview; "GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation."

enforcement. However, Russia soon launched its own extradition request, parading the current and former Russian ambassador into court. As the Sri Lankan justice system attempted to navigate this legal quagmire, the case dragged on, and Manokhin was released on bail. He then fled to Russia where he continues to live with impunity.[165]

I learned that this case represents a pattern whereby Russia attempts to interfere in the extradition process, typically by launching a competing request. Yet, as one prosecutor explained to me, the competing claim is nothing more than a farce:

> I have not seen an example with a competing extradition request where the alleged crime was anywhere close to what we were alleging … We've got an indictment against somebody for causing $15 or 20 million of loss, and the Russians will file something for a $5,000 loss to a babushka somewhere. It's just not on the same level as ours, but they do it pretty regularly in a number of instances.[166]

The real goal is to either repatriate the defendant to safety or delay the extradition process long enough that he is released on bail and can flee.[167]

Extradition interference is not confined to Russia either. Other states, like China, may attempt to retaliate and bully the third country into denying extradition. Thinking back to the Su Bin case, China was far from thrilled that one of their assets might fall into US hands. Merely two weeks after Su Bin's arrest in Canada, Chinese agents invited two Canadian Christian aid workers to a dinner. Little did the aid workers know, it was a trap. The couple was arrested by agents of the Chinese Ministry of State Security and slapped with "mirror image" charges to those against Su Bin.[168] For 19 months, they were held in harsh conditions, sharing a cell of twelve paces by five paces with as many as fourteen prisoners.[169] According to the couple's lawyer, "the Chinese made it clear that the Garratt case was designed to pressure Canada to block Su Bin's extradition to the U.S."[170]

---

[165] "Superpowers Fight It Out Over Russian Hacker in Colombo."
[166] Prosecutor 29, interview, August 13, 2019.
[167] Federal Agent 12, interview, February 12, 2020.
[168] Carlin, *Dawn of the Code War*, 276.
[169] Carlin, 277.
[170] Quoted in Levin, "Couple Held in China Are Free, but 'Even Now We Live Under a Cloud.'"

Extradition interference is particularly problematic since there is no set criteria for countries to prioritize competing requests. As a result, law enforcement "never know how the case will break."[171] In many instances, the outcome is determined by how dependent the arresting country is on the host country versus pursuing country. This provides an advantage to state sponsors. They can employ bargaining strategies, like retaliatory arrests, that pursuing countries bound by ethics and the rule of law cannot employ.[172]

Given that state sponsors will not cooperate and seek to block extradition from third countries, this often leaves law enforcement with one alternative. They must unilaterally ferret the cybercriminal out of their safe haven, which can be accomplished through a lure operation.

In the CRACK99 case, investigators did not believe Xiang Li was working for the Chinese state. However, China has long viewed IP theft as a cheap means to achieve technological growth and close the gap with the US.[173] AUSA Hall elaborated that "whether directly government sponsored or not, Chinese intellectual property theft – even by privateers such as Xiang Li – is state sponsored in the sense that it is encouraged by the Chinese government."[174]

As a result, China would never extradite Li. Another prosecutor explained to me that China also had "zero interest in assisting us in any sort of non-extradition … that would result in the arrest and prosecution in the United States of one of their citizens for cybercrimes committed in mainland China."[175]

The US could not wait for Li to travel either. It was not his custom to do so, and even if he ventured outside China, extradition from a third country introduced risks.

---

[171] Law Enforcement Official 2, interview; Federal Agent 9, interview.
[172] Prosecutor 41, interview; Prosecutor 53, interview.
[173] Hall, interview.
[174] Hall, *CRACK99: The Takedown of a $100 Million Chinese Software Pirate*, 99.
[175] Prosecutor 38, interview.

Agents feared that China would threaten retaliation and the third country might refuse to extradite.[176] If this occurred, Li would know that US law enforcement was onto him and likely never leave the safety of China again. Thus, US law enforcement turned to the lure.

The specter of state sponsorship also hung over the most famous cybercrime case involving a lure. In the early 2000s, US internet service providers, e-commerce websites, and online banks began receiving a series of threats. Hackers had breached their systems and stolen credit card information. If the businesses did not meet their demands, the hackers vowed to publicly release the data or damage the companies' computers. These hackers were simultaneously scamming PayPal by using the stolen credit cards to pay for items on eBay.[177]

However, the case hit a brick wall when law enforcement identified the hackers as Alexey Ivanov and Vasiliy Gorshkov and traced them back to Russia. Cooperation was immediately off the table. The lead prosecutor, former AUSA Steve Schroeder, explained that in two closely related cases, the FBI had sought cooperation from Russia under the 1996 Mutual Legal Assistance Agreement. The requests had been translated into Russian and hand-delivered to the point of contact at the Russian Procurator General's Office. But, the response was always the same: silence.[178] Indeed, AUSA Schroeder recalled, "both Gorshkov and Ivanov told us that they had to be careful in Russia. They didn't fear prosecution. What they feared was that … if [the Russian government] found out what they were doing, they would take over and force them to do the same work for the [government] but [Gorshkov and Ivanov] wouldn't get to keep all the profits."[179] Due to this protection of cybercriminals, the FBI devised a lure operation.

---

[176] Federal Agent 5, interview.
[177] "Russian Computer Hacker Convicted by Jury."
[178] Schroeder, *The Lure: The True Story of How the Department of Justice Brought Down Two of the World's Most Dangerous Cyber Criminals*, 151.
[179] Schroeder, interview.

The hackers had attempted to extort employment from the victim companies. So, law enforcement exploited this opening by contacting the hackers about a job opportunity at a fake start-up computer security company named Invita. The cybercriminals took the bait, and undercover agents informed them that they would need to travel to Seattle for a job interview. Again, the hackers fell for the ruse. They flew to Seattle and during their interview, discussed and demonstrated their hacking accomplishments. At the end, they were presented with handcuffs instead of a job offer.[180]

Although US officials painted a clear picture of the challenges of state sponsorship, any serious researcher would be remiss not to question these observations. There are two significant risks here. The prosecutors and agents I spoke with could be attempting to conceal the use of law enforcement tools to undermine the cyber strength of rival powers. They could also have an incentive to overstate the issues of state sponsorship to justify unilateral US action.

Nevertheless, exploring these alternative explanations, I find several factors that mitigate both concerns. Primarily, the US government is not a unitary actor. Rather, it is composed of various agencies with competing interests and priorities. If the US were merely luring state sponsored cybercrime for geopolitical reasons, one would expect this approach to be championed by the intelligence and national security agencies whose goal is to neutralize rival cyber talent. Yet, those institutions have pushed back against using criminal justice tools to combat this threat. Multiple prosecutors recounted how until 2014 state actors were never charged with cybercrime.[181] They knew that state actors were committing these crimes. However, those cases were handed over to the intelligence community where they "went to a black hole. You never saw them again."[182]

[180] "Russian Computer Hacker Convicted by Jury."
[181] Prosecutor 35, interview; Prosecutor 20, interview.
[182] Prosecutor 20, interview.

This trend reflects a fundamental disagreement within the US government between the intelligence community and USDOJ. One prosecutor explained to me, "The intelligence community would rather leave bad things up because they know where they are and they want to watch them. And the Department Justice, if they see something bad and they can prove it, they want to take it down."[183] The intelligence community was also deeply concerned about the risks that public criminal prosecutions could pose to their highly classified sources and methods. AAG-NSD McCord acknowledged that "if you reveal how you caught [a state sponsored hacker], then they can change their modus operandi and do something different the next time."[184]

As a result, the dominant position within the US government was that its national security interests were better served by maintaining these cases as intelligence rather than criminal justice matters. Nevertheless, as the state sponsored cyber threat increased in prevalence, career USDOJ officials recognized that they could no longer ignore the purely criminal elements of these cases. American companies were suffering devastating losses of IP with "very little recourse."[185] This, combined with the USDOJ organizational culture described above, compelled a law enforcement response and led to the PLA indictment.

Since 2014, the US has continued to prosecute state sponsored cyber activity. While this may appear to support the alternative hypothesis, I learned that the US has remained focused on conduct that crosses the acceptable bounds of espionage. These include indiscriminate data breaches, pilfering trade secrets, and cyber theft and extortion. AAG-NSD John Carlin explained, "We will hold state sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our

[183] Prosecutor 28, interview, January 7, 2020.
[184] McCord, interview, August 6, 2020.
[185] McCord.

goods and breaks our laws."[186] In countries with state capitalism, it can be harder to make this separation between national security activity and commercial crime. However, in the US system, the difference is clearer since the government does not typically own commerce.

For example, in 2015, the US Office of Personnel Management revealed that it had suffered two massive data breaches. This resulted in the compromise of the personal information of 4.2 million current and former federal employees as well as the theft of extremely sensitive data related to background checks and security clearances for 21.5 million individuals. The hacks were attributed to China. But, the US has not pursued criminal charges. This is in line with its approach of not prosecuting cyber conduct that is akin to traditional espionage.

Plus, the US has adopted an even more cautious approach when it comes to applying unilateral alternatives, such as lure operations. As the two case studies in this section reveal, neither lured perpetrator had a direct connection to the state. Law enforcement simply feared that the state would protect these cybercriminals since their actions ultimately benefited the state and/or the state valued their skills.

In fact, the prosecutors I spoke with identified a reluctance to lure state actors since "our intelligence community is very sensitive about operations in countries where they have their own robust operations and something that can screw up their relationships" or ongoing intelligence gathering.[187] This further mitigates against the alternative hypothesis that the US is selectively deploying unilateral alternatives to undermine the cyber talent of rival states. Rather, the US has repeatedly applied lure operations against cybercriminals

[186] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage."
[187] Prosecutor 45, interview.

who are private citizens and located in friendly countries or allies, such as Germany, Romania, Hungary, Vietnam, Malaysia, and the Bahamas.

Nevertheless, these findings still largely stem from US officials who may share a similar worldview. Thus, I sought to cross-reference these revelations by speaking with cybercrime prosecutors from other countries and examining how other nations have responded to US efforts against state sponsored cybercrime. Foreign law enforcement officials largely reiterated the challenges of state sponsorship that US officials shared. Moreover, foreign countries have joined the US in denouncing state sponsored cybercrimes. They have signed onto norms at the G20 against the state sponsored theft of IP. And they have issued public statements to align with US indictments of state sponsored cybercrimes, voicing their agreement that such conduct crossed the lines.

In October 2018, the US indicted seven Russian Main Intelligence Directorate (GRU) officers for international hacking. They targeted international sports and anti-doping agencies to pilfer the medical files of certain athletes. These competitors had been granted exceptions to use prohibited substances for valid medical reasons. The GRU officers then blasted this sensitive personal information of private citizens through social media for the world to see. Their objective was to undermine the credibility of the international doping control system and retaliate for the sanctions placed on Russia over its state sponsored doping campaign.

These hackers also breached the systems of Westinghouse Electric Company to target scientists involved in advanced nuclear reactor development and new reactor technology. Given the nature of this conduct, US Attorney for the Western District of Pennsylvania Scott Brady remarked, “This is not spy versus spy. These were not passive intelligence gathering operations. This is a criminal conspiracy, which caused real harm to real victims. When the GRU targets American corporations to steal trade secrets and

technologies, it costs American companies billions of dollars in lost R&D and capital investment."[188]

The Australian, Dutch, NZ, and UK governments agreed. They all joined the US in denouncing this conduct. The Director-General of the NZ Government Communications Security Bureau affirmed, "These malicious cyber activities serve no legitimate national security interest. They were designed to negatively impact on the ability of people around the world to go about their daily lives free from interference."[189] Likewise, the Canadian government declared, "These acts form part of a broader pattern of activities by the Russian government that lie well outside the bounds of appropriate behaviour, demonstrate a disregard for international law and undermine the rules-based international order."[190]

Even with this international support, many countries still choose to handle state sponsored cybercrime as a military or diplomatic affair. They do not seek to use their criminal justice systems, raising questions about the US approach. However, this may occur since, as AAG-NSD McCord reminded me, prosecuting state sponsored cybercrime "requires coordination and communication between intelligence and law enforcement, which isn't always well integrated in other places."[191]

Knowledge of state sponsored hacking may originate with the intelligence community, which must share this information with law enforcement. These two sides of government must then collaborate as law enforcement seeks to recreate the evidence to prove guilt beyond a reasonable doubt using only unclassified means while protecting the intelligence community's sources, methods, and operations. A Brazilian prosecutor corroborated this explanation and expounded that Brazil has not prosecuted state

[188] Brady, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations."
[189] "Malicious Cyber Activity Attributed to Russia."
[190] "Canada Identifies Malicious Cyber-Activity by Russia."
[191] McCord, interview, August 6, 2020.

sponsored cybercrimes, in part, due to these difficulties of coordination and fear of compromising ongoing intelligence operations.

4.7 Concluding Remarks

This chapter began with an anecdote, seemingly ripped off from a farfetched Hollywood movie script. A cybercriminal is seduced by a beautiful blonde woman. He agrees to visit her in the US only to find out that she is a male US Secret Service agent and that he has been lured to his arrest.

Nevertheless, the law enforcement officials I interviewed explained that lure operations such as this indeed occur. In fact, these conversations suggested that unilateral alternatives are applied more frequently for cybercrime versus other transnational crimes. Since cybercrime is a non-violent offense and capture operations present too many risks, unilateralism has solely manifested in the form of lure operations for cybercrime.

In Chapter 2, I predicted the use of unilateral alternatives in cybercrime would be due to challenges related to the facts of the case, applicable laws, and political considerations. I find that obstacles to cooperation do beleaguer cybercrime cases but primarily stem from factual and political barriers as opposed to legal complications.

Specifically, perpetrators can hide behind the cloak of anonymity of the internet. It remains challenging for law enforcement to not only determine where they are located but also prove beyond a reasonable doubt who was sitting behind the computer. This identification barrier blocks extradition, quasi-extradition, and waiting for defendants to travel. But, it can be resolved through a lure operation, regardless of where they are located. Once the cybercriminal arrives on a lure, they cannot plausibly deny their culpability. Plus, they typically carry their devices, providing a treasure trove of evidence.

Additionally, the remote nature of cybercrime removes the need for perpetrators to step foot in the victim country or travel. They can operate from anywhere in the world.

This means they generally cannot be arrested in the victim country or while travelling. It also means they can choose to shelter indefinitely in safe havens. Therefore, a unilateral response is required to ferret them out.

But, why have certain countries become cybercrime safe havens? I learned that legal barriers do not meaningfully impede securing custody. Dual criminality is no longer an obstacle to extradition. In fact, the Budapest Convention has adequately promoted the outlawing of cybercrime globally while building a community of cooperation and trust. Cybercriminals also cannot skate on claims that their conduct was a political offense. This defense is typically undermined by the commercial nature of most cybercrimes. Furthermore, pursuing countries have not clashed in jurisdictional battles that would require the use of unilateral alternatives.

Rather, cybercrime faces political challenges that create a need for unilateralism. Certain states lack the political will to cooperate in rendering these offenders. Local politicians recognize they can score domestic political victories by standing up to the pursuing country and denying assistance. Cybercrime makes it easier to do this. The perpetrators avoid targeting victims in their home country. The crimes seem less serious. And, the offenders can elicit greater public sympathy.

Other countries take this a step further by serving as state sponsors. They recognize the value of cybercrime for accomplishing state objectives, so they shelter and sometimes even coopt profit-motivated cybercriminals. When these perpetrators travel and are arrested, state sponsors likewise seek to meddle in the extradition process to protect them.

Despite these findings, we must remain cautious. My core set of interviewees consisted of US law enforcement officials. These individuals may represent a homogeneous worldview. They also may have incentives to present the US in the best light and exaggerate certain challenges to justify unilateral US action. Throughout this

chapter, I have sought to mitigate these concerns by triangulating the revelations of my interviews with court records and media reporting. I have also spoken with cybercrime prosecutors from other countries, who shared similar insights, providing greater confidence in my findings.

There is another concern that the US may simply be using unilateral alternatives for national security purposes to take out the cyber talent of rival powers. However, we have learned that the US has focused on prosecuting cases where state sponsored cyberattacks cross the acceptable bounds of espionage, such as by stealing IP for commercial advantage. The US has been joined by other nations in agreeing to norms on this distinction between legitimate national security activity and criminal conduct and in calling out such illicit behavior.

The alternative hypothesis is further mitigated by the fact that the US is not a unitary actor and the national security apparatus, whose goal is to counteract foreign cyber talent, has pushed back against the use of law enforcement tools here. They prefer to track and monitor state sponsored cyber threats. In fact, the known lure operations have only been used against profit-motivated cybercriminals, not state actors.

The findings in this chapter now raise the question, how does the experience of cybercrime compare to other transnational crimes? Moreover, what lessons can be applied from these offenses to cybercrime? Both questions will be explored next.

5. COMPARING CYBERCRIME TO OTHER TRANSNATIONAL CRIMES

"Benghazi Attacks Suspect is Captured in Libya by U.S. Commandos."[1] "Attorney Says Client was Kidnaped; Wants Drug Charges Dropped."[2] "Chinese National Arrested in Carbon Fiber Smuggling Sting."[3] Ripped from the headlines, prosecutions such as these raise the question: is the use of unilateral alternatives to extradition for cybercrime really that distinctive? Or, is cybercrime merely a form of old wine in new bottles, similar to other transnational crimes in this respect? How can we therefore anticipate that cybercrime enforcement will develop?

Through my interviews with federal law enforcement officials, I seek to shed light on these questions. Specifically, I compare cybercrime to four main areas of cross-border criminality: terrorism, drug trafficking, fraud and foreign corruption, and export control and sanctions violations. I also explore what lessons can be applied from the prosecution of each of these offenses to cybercrime.

These four offenses were selected since they are the most prosecuted transnational crimes where the lead perpetrators are generally located abroad. Additionally, they each could experience similar obstacles as cybercrime. For instance, terrorism and drug trafficking cases could suffer from attribution challenges, and the leaders of these organizations could shelter indefinitely in safe haven countries. Likewise, terrorism, drug trafficking, foreign corruption, and export control could all be inhibited by the host country protecting the perpetrator. Furthermore, host countries could lack the political will to cooperate on fraud cases since these are non-violent crimes and often only harm companies, which are unsympathetic victims. Therefore, each of these four crimes could

[1] Goldman and Schmitt, "Benghazi Attacks Suspect Is Captured in Libya by U.S. Commandos."
[2] Reza, "Attorney Says Client Was Kidnaped; Wants Drug Charges Dropped."
[3] "Chinese National Arrested in Carbon Fiber Smuggling Sting."

face a similar need for unilateralism as cybercrime and accordingly present useful settings to examine the potential robustness of my findings over time.

Indeed, I found that all transnational crime prosecutions rely on unilateral alternatives at times. However, my interviews revealed that for other cross-border offenses, either host countries have a greater interest in combatting the illicit conduct or the perpetrators are more prone to travel on their own. This latter aspect enables offenders to be arrested in and rendered from friendlier jurisdictions. Therefore, there is less of a need for unilateral alternatives to extradition in each category of cross-border criminality relative to cybercrime.

To combat terrorism, the US adopted a leading role by taking unilateral action. In the early years following the September 11 terrorist attacks, the US was on a "quasi war footing" and primarily handled terrorism as a military or intelligence affair.[4] It was generally not considered a criminal justice matter. Indeed, one prosecutor lamented to me that terrorists "arrested at the battlefield present so many evidentiary issues that they are usually turned over to the locals or sent to Guantanamo but not domestically prosecuted in the US."[5]

However, by the mid-2000s, this approach began to change. Foreign countries objected to the US's use of detention facilities, such as Guantanamo Bay, and military tribunals due to reports of widespread torture and human rights abuses. As the US faced those external pressures and moved further away from that quasi war footing, the law enforcement response took center stage.[6] These cases then presented less of a need for unilateralism. The US preferred for the perpetrators not to be brought to the US to stand

[4] Prosecutor 31, interview, September 16, 2020.
[5] Prosecutor 15, interview.
[6] Prosecutor 31, interview, September 16, 2020.

trial, so they instead relied on prosecutions abroad. Why? These individuals posed a significant risk of radicalizing other inmates once incarcerated in US prisons.

While there is a small handful of exceptions involving unilateral capture operations, those terrorism prosecutions where the US has sought to secure physical custody over the offender have predominantly been resolved cooperatively. Host countries either successfully extradite terrorists or hand them over through a quasi-extradition.

As Dan E. Stigall, the Deputy Chief of Staff and Counsellor for International Affairs for the National Security Division (NSD) of the US Department of Justice (USDOJ), explained, terrorism has been near universally condemned by the international community. In addition, the effects of terrorism, which frequently involves very public acts of violence, are typically easier to discern and more immediately and acutely felt than the effects of cybercrime. Likewise, attribution is often easier in the case of terrorism as many terrorist groups seek credit and acclaim for their violent activity. Cybercrime, in contrast, takes place in cyberspace, and its perpetrators generally seek to remain hidden in the shadows. These differences between terrorism and cybercrime mean that it is often easier to galvanize international action against terrorist actors and facilitate international cooperation vis-a-vis terrorism.[7]

However, cybercrime cases are not likely to follow either path seen in terrorism cases. The lack of international consensus on cybercrime combined with the benefits of this conduct to host countries preclude relying on them to domestically prosecute or cooperate in rendering the perpetrators. At the same time, the most prolific cybercriminals reside in governed spaces, like Russia and China. So, David Kris, the former USDOJ-NSD

[7] Stigall, interview, November 4, 2020. Stigall formerly served as Director for Counterterrorism of the White House National Security Council (2017-2019), Trial Attorney for USDOJ's Counterterrorism Section (2016-2017), Counsel to the NSD Assistant Attorney General (2015-2016), and Trial Attorney for USDOJ's Office of International Affairs (2009-2015).

Assistant Attorney General (AAG) from 2009 to 2011, remarked to me, "we're not going to send the special forces into China to arrest a cybercriminal."[8]

Even though these offenders may be state sponsored, they are not currently engaged in any type of cyber war. These perpetrators thus fall short of being considered enemy combatants, and the law of armed conflict would not apply. From both a legal and diplomatic perspective, these factors would generally preclude a unilateral capture operation. Plus, given the international condemnation of Guantanamo Bay, cybercriminals are not likely to be shipped off to a similar facility outside the criminal justice system where they could be subject to indefinite detention or human rights abuses.

Similar to terrorism, drug trafficking experienced a prolonged period of unilateralism. Due to weak judicial systems and constitutions unfriendly to extradition, drug traffickers lived in host countries with virtual impunity. So, US agents and their proxies sometimes kidnapped and allegedly tortured defendants to bring them to the US for trial. This unilateralism marked the 1970s, 80s, and 90s.

Nevertheless, as the 20th century came to an end, a sea change arose in transnational drug trafficking cases. Prodded by domestic political pressures and US foreign aid, the most prolific host countries undertook dramatic reforms. They updated their laws and in the case of Colombia, "started extraditing left and right."[9] Host countries have generally recognized the harmful impacts that drug trafficking causes, both domestically and internationally. So, they have acted on this shared interest and cooperated. As a result, prosecutors reported that the US has not again turned to a unilateral capture operation in a drug trafficking case.[10]

[8] Kris, interview.
[9] Prosecutor 39, interview.
[10] Avergun, interview, August 21, 2019.

At times, cooperation in drug trafficking cases has indeed been stymied by corruption. The degree of poverty in the most prolific host countries combined with the large sums of illicit proceeds generated by these crimes create a ripe opportunity to purchase the protection of local officials. However, even when corruption has proved vexing, prosecutors reported that they still have successfully worked with the host country rather than resorted to unilateralism. This typically occurred through the creation of vetted law enforcement units. Plus, drug traffickers often travel to expand their business networks.[11] Thus, they can be arrested in other jurisdictions where corruption is less of a concern, again obviating the need for unilateralism.

Despite the transformation witnessed in drug trafficking cases, the obstacles to bringing cybercriminals to justice are not legal in nature. Therefore, they cannot be solved through legal reforms in the most prolific host countries. The strained geopolitical relationship with these countries likewise precludes using foreign aid in the same way to incentivize cooperation. Host countries also do not share an interest in ending cybercrime since, unlike drug trafficking, it has little to no destructive effects on their homeland.

While it is possible that cybercriminals, like drug traffickers, may turn against their home country, such a change is not probable. Perpetrators currently have a vast victim pool abroad with opportunities to make untold profits. They simply have little reason to target their fellow citizens. And, their home countries have already made an example out of those who harm domestic victims. This sends a clear message that cybercriminals can live with impunity if they target foreigners. But, they better not dare attack their fellow countrymen, or they will be met with swift justice.

Cybercrime does face similar challenges as drug trafficking with respect to bribery. It generates large sums of illicit proceeds and occurs in locations like Russia and Ukraine

[11] Avergun, interview, September 25, 2020.

that suffer from high levels of corruption and/or poverty. Yet, the same cooperative approach used in drug trafficking investigations cannot be reliably employed here. Host countries either do not have the same interest in bringing the perpetrators to justice or sponsor this conduct. This mitigates any incentives for them to form vetted units. Plus, cybercriminals do not travel as part of the conspiracy like drug traffickers. Consequently, law enforcement cannot simply wait for them to leave their home country.

With respect to fraud and foreign corruption, there is again less of a reliance on unilateral alternatives. These defendants tend to be international executives. Their livelihoods often depend on conducting business across borders, which means they can be arrested while travelling. They are also more willing to hand themselves over to avoid an extradition request or Red Notice impeding their travel. Even if they do not travel, these offenders typically reside in countries that will cooperate through the extradition process.

Additionally, unilateral alternatives are simply less viable here. Prosecutors are accusing these individuals of making material deceptions. But, the perpetrators can argue that the government has also engaged in material deceptions by luring them, turning the jury against the prosecution. Given that these offenders can almost always be extradited or arrested while travelling, a lure operation would thus introduce unnecessary risks.

The experience of fraud and foreign corruption contrasts with that of cybercrime. Cybercriminals can continue their illicit conduct without any need to leave their home country and do not generally travel on their own. This means there is less of a reason for them to self-surrender and less of a chance to intercept them in transit. They also know that they can challenge their extradition, particularly over attribution, which further limits their incentives to self-surrender. So, we are not likely to witness an outcome similar to fraud or foreign corruption cases. Rather, law enforcement is often faced with no choice but a lure to ferret out cybercriminals, even if such a tactic may introduce risks at trial.

Alternatively, export control and sanctions prosecutions face similar political challenges to cybercrime. In both instances, the host country benefits from and actively sponsors these forms of criminality. Therefore, they pull out all the stops to protect perpetrators and provide safe haven. This even means interfering in extradition requests when defendants are arrested in third countries. As a result, law enforcement frequently must turn to unilateral lure operations.

Given the shared political impediments, export control and sanctions cases suggest that cybercrime cases will necessitate a sustained use of unilateral alternatives. This is frequently the only way to overcome the political barriers and smoke out these individuals. In fact, the need for such tools is likely to be even higher for cybercrime. As part of the conspiracy, export control and sanctions defendants often must cross borders to inspect merchandise, finalize deals, and deliver the illicit goods. This presents a viable opportunity to wait and arrest them in more cooperative jurisdictions. However, there is no comparable business reason for cybercriminals to travel. They can also hide behind their cloak of anonymity, the internet. Both challenges may only be overcome with a lure operation.

These comparisons between cybercrime and other transnational crimes do not suggest that international cooperation will meaningfully develop in this space. Instead, they foreshadow a world increasingly requiring unilateralism to achieve justice.

This chapter proceeds as follows. In the first four sections, I compare cybercrime to each type of transnational crime, beginning with terrorism, then drug trafficking, then fraud and foreign corruption, and finally export control and sanctions violations. In each section, I trace the evolution of the methods used to secure custody over perpetrators of these other offenses and examine how the need for unilateralism compares to cybercrime. I also contemplate whether cybercrime is likely to develop in a similar manner as those other crimes. The last section restates my key conclusions.

5.1 Terrorism: Moving from a Quasi War Footing to Criminal Prosecutions

I first examine the lessons that can be learned from efforts to combat terrorism. I discovered that in the early years, the US was on a quasi war footing and thus relied on military solutions instead of alternatives to extradition. Even as the US moved to focus on a criminal justice response, it generally has not turned to unilateralism. It has preferred for other countries to prosecute. Host countries have also been willing to hand over terrorists due to the international consensus and strong political will to fight this threat.

Nevertheless, countries are unlikely to rely on comparable military solutions, such as drone strikes and capturing perpetrators for indefinite detention, in cybercrime. Unlike terrorists, cybercriminals live in governed spaces, which would create a high risk of retaliation. Plus, the law of armed conflict does not apply and could not similarly justify such actions under international law. The cooperative route is not likely either since countries do not have the same level of interest or consensus in cybercrime.

It was midnight on June 14, 2014. Libyan terrorist Ahmed Abu Khatallah just returned to a one-bedroom beachside villa on the outskirts of the city of Benghazi. He had spent the day skirmishing with military forces.[12] Out of the darkness emerged an eight-man team of US military commandos. Within minutes, Abu Khatallah was thrown to the ground, disarmed, and knocked into submission. Now in custody, he was led down a 500-meter walk to the coast and placed on an amphibious transport vehicle for a two-hour journey to the USS New York. That warship would be his home for the next thirteen days until he reached the US where he would stand trial.[13]

Abu Khatallah was accused of orchestrating a terrorist attack on the US consulate in Benghazi. On September 11, 2012, assailants attacked the consulate with automatic

[12] DeYoung, Goldman, and Tate, "U.S. Captured Benghazi Suspect in Secret Raid."
[13] Hsu, "Benghazi Terror Suspect Is in U.S. Court. So Is an FBI Agent Who Captured Him."

weapons and rocket-propelled grenades, setting it ablaze. During the assault, they killed the US Ambassador to Libya and a US State Department employee. The next morning, the fighting continued as terrorists turned their attention to a Central Intelligence Agency annex, killing two contractors in a mortar blast.[14]

The Abu Khatallah case would seem to match the stereotypical picture of US efforts to combat transnational terrorism. Commandos swoop into a foreign jurisdiction, unilaterally capture the perpetrator, and whisk him out from impunity. However, this case stands out from the others. It is one of the few that involved a capture operation to bring the defendant back to stand criminal trial in the US.

In fact, capture operations in terrorism have not typically been applied as alternatives to extradition. They have been predominantly used for military or intelligence purposes rather than to accomplish criminal justice objectives.

Following the September 11 terrorist attacks, the US was catapulted onto a quasi war footing. Given the immediate danger that terrorists posed, the priority was to protect American citizens and servicemembers. One prosecutor explained to me that the impact of the case on the Department of Defense, Central Intelligence Agency, and foreign intelligence services "drove the decision" on how to proceed.[15] Another prosecutor agreed, stating that the "priorities were more about securing the individual and getting the intelligence, which could take a very long time."[16] Such emphasis would enable the US to both remove a threat actor and potentially disrupt future attacks by their associates.

Nevertheless, this approach came at a price. In a criminal trial, prosecutors must always consider how the defendant was treated and the state of the evidence to avoid any constitutional challenges.[17] Yet, there was often a desire, for example, to avoid providing

[14] DeYoung, Goldman, and Tate, "U.S. Captured Benghazi Suspect in Secret Raid."
[15] Prosecutor 32, interview.
[16] Prosecutor 15, interview.
[17] Prosecutor 31, interview, September 16, 2020.

terrorists with a Miranda warning that they had a right to counsel. If they were aware of this right, they would likely be less willing to talk and provide the needed intelligence. But, without a proper Miranda warning, any statements the offender made could not be used as evidence. Plus, the defendant could challenge his arrest, as Abu Khatallah did since he was interrogated for several days before receiving a Miranda warning.

As a result, one prosecutor recollected that in the early 2000s, transnational terrorism cases were considered a military issue. Accordingly, they were dealt with using military tools, such as military tribunals.[18] Another prosecutor similarly recalled that typically, terrorism defendants captured on the battlefield were immediately placed into the military system.[19] These prosecutors may have had incentives to downplay the use of such military mechanisms given their controversy under international law. However, their willingness to readily acknowledge the leading role of these tools lends credibility to their recollections.

In the mid-2000s, this approach all began to change. European allies strenuously objected to the US's use of facilities such as Guantanamo Bay due to concerns over the inhumane treatment, torture, and indefinite detention of prisoners. In fact, many countries would not cooperate with the US unless the US provided assurances that the terrorist would not be sent to Guantanamo. Due to these external pressures and as the US moved further away from its initial quasi war footing, law enforcement began working with the military to collect evidence and build criminal cases. This transformation was accelerated by the Obama administration's decision to close Guantanamo Bay and the CIA's secret interrogation and detention facilities known as black sites. It was then cemented by prosecutors' desires to pursue these cases criminally and not see Guantanamo reopen.[20]

[18] Prosecutor 31, interview, August 16, 2019.
[19] Prosecutor 21, interview.
[20] Prosecutor 31, interview, September 16, 2020.

Nevertheless, military solutions still have a place in combatting terrorism. Rather than capturing terrorists for indefinite detention or military tribunals, the US has now turned in certain cases to military drone strikes. For the purposes of this analysis, drone strikes are not considered an alternative to extradition since their goal is not to bring the fugitive to justice in the pursuing country's courts. However, since they are another potential tool to combat the terrorist threat, they may impact the use of unilateral alternatives to extradition. Indeed, former Acting AAG-NSD Mary McCord elaborated that a capture operation "puts US lives at risk … because they can get shot and killed really easily. And so, the stakes are far higher in a capture operation to US person lives, US military lives, and law enforcement lives."[21] Drone strikes mitigate this risk while still neutralizing the terrorist threat.

Alongside these military operations, criminal prosecutions have indeed become a more important tool in the fight against terrorism. Yet, I discovered that they have faced less of a need for unilateralism. Primarily, the US has preferred for the terrorist's country of citizenship or the country where the attack took place to prosecute. One prosecutor shared with me that the "US interest isn't in bringing every terrorist to the US to prosecute."[22] For example, after the bombing in Kampala during the World Cup, the US deferred to Uganda to prosecute and sent US prosecutors there for four to five years to assist local authorities in building the case. This decision was made even though there were US victims and the US had jurisdiction to press charges.

Prosecution in a foreign court may not always produce the same outcome as if the defendant had been tried in the US. The US has relatively harsh sentences for terrorism, so perpetrators may receive less jail time abroad. However, a prosecutor explained to me that

[21] McCord, interview, August 14, 2019.
[22] Prosecutor 31, interview, September 16, 2020.

the possibility of a lesser sentence would not change whether the US assisted in the case or believed deferring to the other country was the right decision.[23]

Given the high political salience of combatting terrorism, this stance seems counterintuitive. What is the rationale? I learned that US law enforcement had serious concerns about incarcerating foreign terrorists in US prisons. These individuals typically do not deradicalize after being apprehended. So, they could radicalize other inmates, particularly those nearing release. Likewise, terrorists generally do not receive life sentences.[24] Once released, other countries typically refuse to accept these individuals. This leaves the US with the dilemma of what to do with them.[25] If discharged in the US, they could return to their old ways. A prosecutor I interviewed recounted a case where a foreign terrorist was convicted in the US. He only received a 10-year sentence and soon began attempting to recruit and train fellow prisoners to join the Islamic State (ISIS).[26]

Despite this preference for foreign prosecution, there have still been certain cases where the US interest has been compelling enough to pursue a domestic prosecution. I heard from prosecutors that custody over these perpetrators has generally been secured cooperatively, not unilaterally. These prosecutions have almost exclusively proceeded through quasi-extradition or extradition.[27]

One prosecutor explained that host countries often had the political will to assist. They had a shared interest in protecting their homeland from terrorism and did not want these offenders running free in their territory. Yet, these countries feared possible reprisal attacks for extraditing a terrorist. As a result, they would use informal means, such as an

[23] Prosecutor 31.
[24] Prosecutor 31, interview, August 16, 2019.
[25] Prosecutor 31, interview, September 16, 2020.
[26] Prosecutor 31.
[27] Prosecutor 15, interview; Prosecutor 31, interview, August 16, 2019.

expulsion. These techniques would enable them to quietly render the terrorist, who was generally not one of their citizens, and avoid any political blowback.[28]

In addition to fears of retaliation, quasi-extraditions have been used more frequently in terrorism cases due to the location of defendants. They more often reside in less developed countries that may not have the judicial processes to support a formal extradition.[29] Since these countries have the political will to assist, they can instead resort to informal methods.

When terrorists have been located in Western countries, the US has then pursued formal extraditions. These requests have been "uniformly successful."[30]

Prosecutors acknowledge that there is widespread consensus regarding the criminality and severity of terrorism, which greases the wheels of cooperation.[31] One prosecutor elaborated that terrorism cases are "easier because the consequences and the nature of the actions is more black and white in people's minds … Countries will pull out all the stops to help one another."[32] As USDOJ-NSD Deputy Chief of Staff and Counselor for International Affairs Dan E. Stigall explained, "countries will not generally try to excuse this behavior."[33] He elaborated that while some states do use terrorists as proxies to project force, state supported cybercriminals are often more difficult to incapacitate. This is because, while terrorists frequently must travel abroad to plan and conduct physical attacks, state sponsored cybercriminals may ply their trade remotely with greater facility and can therefore shelter in the safe haven of their sponsor country.[34]

[28] Prosecutor 32, interview.
[29] Prosecutor 15, interview.
[30] Prosecutor 32, interview.
[31] Prosecutor 23, interview.
[32] Prosecutor 23.
[33] Stigall, interview, August 15, 2019.
[34] Stigall, interview, November 4, 2020.

Indeed, certain terrorism prosecutions, such as the Abu Khatallah case, do involve unilateral capture operations. Nevertheless, due to the factors outlined above, there is simply less of a need for such a unilateral approach. So, seizures are only used for a "very small subset of cases. It would be very rare to go into countries for a capture" for criminal justice purposes.[35] Another prosecutor similarly remarked to me that "seizure is always a last resort. We would always like to go through a normal extradition."[36]

These findings raise two concerns. First, there may be a selection bias whereby the US is only prosecuting those terrorists on whom it can easily lay hands. It may be leaving the rest for foreign countries to prosecute or military drone strikes to neutralize. Nevertheless, prosecutors shared with me that the decision to pursue US criminal charges depends on whether there are direct US victims and how compelling is the US interest. It does not depend on the ease of securing custody over the perpetrator. One prosecutor quipped that if the US simply wanted to inflate numbers and win easy cases, it could have brought over hundreds of ISIS terrorists held by the Syrian Democratic Forces.[37] Likewise, the US has pursued criminal prosecutions in difficult cases and not just turned to drone strikes. The Abu Khatallah prosecution provides a perfect example. It required extraordinary steps to secure custody, yet the US deemed there was a compelling interest in placing him on trial in a US courtroom.

Second, given the international controversy surrounding captures, prosecutors may have an incentive to downplay their frequency. However, a capture operation would generate significant media attention. Since these defendants would know they were captured and would be publicly tried in criminal court, they would likely challenge the circumstances of their arrest. There would likely be testimony from the federal agents

[35] Prosecutor 31, interview, August 16, 2019.
[36] Prosecutor 11, interview.
[37] Prosecutor 31, interview, September 16, 2020.

involved in the seizure. This publicity would then enable media and nongovernmental organizations to report on and track the use of such captures. Human Rights First has done precisely that. From September 2001 to December 2016, they found that 113 terrorists were rendered from abroad to the US for criminal prosecution. Yet, only one case involved a seizure.[38] My review of all US terrorism criminal prosecutions since then uncovered that only two others, including Khatallah, have been subject to capture operations.

Even if there was a need for unilateralism here, prosecutors explained to me that less drastic unilateral measures, such as lure operations, are simply less viable in terrorism cases. Lures can pose serious public safety threats if law enforcement loses track of the terrorist once he arrives in the country. So, pursuing countries are less likely to take such a risk.[39] Prosecutors also reported that the US faces particular difficulty with lures for terrorism due to the US's negative global image over its previous policy of extraordinary rendition. As a result, third countries are less willing to assist on lure operations or serve as the lure destination in terrorism cases, once again limiting the viability of this alternative.[40]

These findings now raise the question, can we expect any similar outcomes for cybercrime prosecutions?

Well, the most prolific cybercriminals operate from sovereign territories with functioning governments, such as China, Iran, North Korea, and Russia. This contrasts with terrorism cases where most perpetrators resided in denied or ungoverned areas. As a result, the US was able to employ seizures in those locations.[41] As AAG-NSD McCord shared with me, the US resorted to a capture operation in the Khatallah case since there was "no functioning government" in Libya at the time.[42] In fact, the US has almost

[38] "Identified Foreign Captures."
[39] Prosecutor 32, interview.
[40] Prosecutor 24, interview.
[41] Kris, interview.
[42] McCord, interview, August 14, 2019.

exclusively conducted capture operations of terrorists in ungoverned spaces.[43] If a terrorism suspect was located in an area with a functioning government, AAG-NSD Kris noted that the US generally would not pursue a seizure.[44]

Given the differences in locations of residence, a capture operation or drone strike would therefore be precluded for most cybercrime cases. This disinclination to employ such tools in governed spaces is for both legal and political reasons. Specifically, international law provides greater flexibility for capture operations or drone strikes in locations without functioning governments. Dan E. Stigall observes that the international community has grown tolerant of limited incursions into ungoverned spaces to counter terrorism. He explains the rationale for these more flexible rules on the use of force: "When authorities of a fragile state cannot effectively counter an empowered non-state armed group operating in their own territory that poses a threat to international security or the larger world, such as a terrorist organization, capable states should be able to act decisively to counter it in their stead, if only out of a need for self-preservation."[45]

From a political perspective, a capture operation or drone strike involving a country with a functioning government poses a sizeable risk for escalation. It could even be seen as an act of war. In contrast to terrorism, the most prolific host countries for cybercrime would have the technical capacity and organization to meaningfully retaliate. China, Iran, North Korea, and Russia not only possess conventional military strength but also the resources to conduct offensive cyber operations.

This means that in response to a capture of one of their cybercriminals, they could unleash cyberattacks on government sites, businesses, and critical infrastructure. We only need to look at the 2007 cyberattacks on Estonia to see how such retaliation could play

[43] McCord.
[44] Kris, interview.
[45] Stigall, "Counterterrorism, Ungoverned Spaces, and the Role of International Law," 51.

out. In April of that year, the Estonian government decided to move a Soviet war memorial to a cemetery on the outskirts of town. Within days, the country came under a crippling distributed denial of service attack originating in Russia. The attack took down the websites for the nation's parliament, banks, newspapers, and broadcasters: "cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news."[46]

Despite its impressive cyber capabilities, the US is not immune to this type of retaliation. The prosecutors I interviewed, including former Deputy Attorney General Rod Rosenstein, repeatedly emphasized that it is impossible to prevent cyberattacks.[47] The internet was not designed with the threat of malicious actors in mind. So, it is chockfull of vulnerabilities that can only be rectified by reinventing the internet from the bottom up. Additionally, even the best cyber defenses can do little to address the human factor. All it takes is one employee to click on a malicious link in a spam email to provide hackers with access to sensitive networks.

Plus, a cyberattack in retaliation for a capture operation could rely on a zero-day exploit. These "crown jewels in the cyber realm" are often used by state sponsors "to conduct high-level espionage and prepare military attacks on unsuspecting targets."[48] By their very nature as unknown software vulnerabilities, these attacks are incredibly difficult to prevent.

A country like the US is also not immune to retaliation due to its global stature and capacity to engage in further escalation. State sponsors have already demonstrated a willingness to launch cyberattacks on US critical infrastructure without any pretext, let

[46] McGuinness, "How a Cyber Attack Transformed Estonia."
[47] Rosenstein, interview.
[48] Carlin, *Dawn of the Code War*, 181.

alone in response to a capture operation. In 2013, a network engineer for a company with ties to the Iranian Revolutionary Guard hacked into the supervisory control and data acquisition system of New York's Bowman Dam. Had the dam's sluice gate not been manually disconnected for repairs, the Iranian hacker could have exploited this access to operate and manipulate the sluice gate and flood local homes.[49] While New York's Bowman Dam is only 20-feet-tall, prosecutors posited that the Iranian hacker intended to gain access to the 245-foot-tall Arthur R. Bowman Dam in Oregon, which held back a 3,500-acre reserve.[50] AAG-NSD Carlin recalled that other state sponsors were seeking to obtain this same level of access and had a real fear that if they "achieved the type of access that Iran had at the Bowman dam, they might pull the virtual trigger."[51]

Carlin's observation of the threat is not an exaggeration either. We have already seen examples where the Russian Main Intelligence Directorate (GRU) has launched audacious cyberattacks against the US. One of the most stunning was its hack into the computer networks of the Democratic Congressional Campaign Committee, Democratic National Committee, and presidential campaign of Hillary Clinton. The GRU's goal was to release damaging information and interfere in the US elections. Even more concerning, the GRU "conspired to hack into the computers of state boards of elections, secretaries of state, and US companies that supplied software and other technology related to the administration of elections to steal voter data stored on those computers."[52]

Countries like Russia can take such provocative actions in cyberspace since it is difficult for victims to fight back. As we learned in Chapter 4, attribution remains a pressing challenge. Countries perpetrating cyber offenses can route their attacks around

[49] Carlin, 229.
[50] Prosecutor 28, interview, January 7, 2020; Carlin, *Dawn of the Code War*, 229.
[51] Carlin, *Dawn of the Code War*, 229.
[52] "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," July 13, 2018.

the world and throw up false flags. Consequently, it may take years to determine the culpable party and even then, the accused state may still assert that some other dude did it. Therefore, if a host country were to launch a cyberattack in retaliation for a capture operation, it would be hard for the arresting country to escalate further, leaving the host country with little to fear. Indeed, the US response to the GRU election hacks, which hit at the core of American democracy, was merely a USDOJ indictment followed by sanctions.

Retribution could also be more indirect than a cyberattack. The host country could retaliate against corporations from the pursuing country that operate within its territory. Or they could undermine other aspects of the diplomatic relationship on issues such as trade or climate change. They could even arrest residents or visitors who are citizens of the pursuing country on trumped-up reciprocal charges. We have already seen this happen in response to mere extraditions of cybercriminals from certain countries. So, it is no stretch of the imagination to envision them doing the same in response to a capture operation.

The risk of retaliation is less pronounced for a lure operation. Unlike being snatched off the street, the defendant may never know he was lured. The government has no obligation to disclose this fact at trial. In fact, the secrecy surrounding lures presented one of the greatest challenges to this research since prosecutors and agents were often reticent to acknowledge the use of that tool in specific cases. Considering the clandestine nature of these operations, the host country may simply think the cybercriminal slipped up and was arrested while travelling, which may mitigate their incentives to retaliate.

Plus, the infringement on the sovereignty of the host country is minimized with a lure. While such an operation involves deceiving one of their citizens, it does not involve sending military or law enforcement officials into their territory like in a capture operation. And it does not involve dropping a bomb within their borders like a drone strike, which can endanger civilian lives and infrastructure. Therefore, the risks of reprisal for a lure

operation are diminished as compared to a seizure or drone strike. In fact, the US has not yet suffered retaliation for any of the publicly documented lure operations in cybercrime.

Another distinction between terrorism and cybercrime is that currently, no pursuing country is on a cyber war footing. Therefore, the law of armed conflict does not apply, and the cybercriminals that are the focus of this analysis cannot be considered enemy combatants. The US relied heavily on the law of armed conflict and the status of terrorists as unlawful enemy combatants as legal justification for their capture, detention, and disposal through the military system. However, the cybercrimes targeted for criminal prosecution have fallen far short of cyberwarfare. It would be quite the stretch to consider online fraudsters, burglars, and extortionists to be enemy combatants or for the law of armed conflict to apply. Thus, military detention or drone strikes could not be accordingly justified here.

Even if the cyber threat evolves into cyberwarfare, the international upheaval in the mid-2000s against the Guantanamo Bay system, which pressured the US to transition to a criminal justice approach, suggests that a pursuing country would not repeat the mistakes of the past. Otherwise, they would significantly risk losing the support of their allies. This assistance is particularly crucial for combatting cybercrime given the global nature of these offenses with evidence spread around the world.

Cybercrime has also not posed any significant threat to human life, which mitigates against deploying a capture operation or drone strike. Even if the cyber threat becomes more violent, the incentives for a pursuing country to use such an extraordinary tool remain counterbalanced by the location of the perpetrator. A certain amount of technological infrastructure is required to commit cyberattacks. So, these offenders will likely continue to reside in governed spaces. Therefore, the risk of retaliation from the host country and backlash from the international community for invading the sovereignty of a

foreign power remain. This suggests that a capture operation or drone strike would only be used in the most extreme of cases, the so-called electronic Pearl Harbor.

Equally important, cybercrime is not likely to follow the cooperative path. In terrorism, host countries recognized the threat that perpetrators posed to their national security and the safety of their citizens. In cybercrime, there is no such international consensus on the seriousness and wrongfulness of this conduct. The offenders may pose no threat to the host country's citizens since they typically only target foreign victims. And the stakes of denying cooperation may not seem as high to the host country, particularly as compared to terrorism. So, they can afford to stand up to the pursuing country to gain a domestic political win. The host country may also benefit from cybercrime as it stimulates their economy through illicit proceeds and perpetrators can be coopted to accomplish state objectives. For these reasons, host countries do not have the same incentives to cooperate via a domestic prosecution, quasi-extradition, or extradition as they do for terrorism.

Yet, pursuing countries wish to lay their hands on cybercriminals and prosecute them through their criminal justice system. Unlike terrorism, these individuals pose little to no public safety risk once incarcerated. Rather, such prosecutorial efforts send a message to other cybercriminals that they are not safe from justice and serve as a deterrent.[53] With cooperation and military options both frequently off the table, this thus leaves pursuing countries with a greater need for unilateral lure operations.

5.2 Drug Trafficking: Transformation from Unilateralism to Cooperation

I now consider the comparison between cybercrime and drug trafficking. Inadequate legal and judicial institutions in key host countries led to an initial use of unilateral alternatives in drug trafficking cases. However, the inauguration of legal reforms and conditions of US foreign aid soon catalyzed cooperation. Indeed, many host countries

[53] Prosecutor 14, interview.

have the political will to combat drug trafficking due to its harmful domestic impacts. And drug kingpins travel as part of the conspiracy, so they can be arrested and extradited from third countries. There also tends to be less of an urgency to arrest drug traffickers since they can easily be replaced in the conspiracy, limiting the need for unilateral tools.

However, this transformation is not likely to occur in cybercrime. The challenges of cooperation are not legal in nature. Cybercriminals also know better than to target their fellow citizens. This mitigates their home countries' political will to lend a hand. Nor do cybercriminals travel as part of the conspiracy, so they cannot be arrested in third countries. Yet, there is an urgency to lay hands on the individuals behind a cybercrime since this can immediately end the attack.

Let's flash back to January 6, 1973. According to Francisco Toscanino, he was at his home in Montevideo, Uruguay when his telephone rang. On the other end was Hugo Campos Hermedia, a member of the Montevideo police. Hermedia lured Toscanino to meet him near a deserted bowling alley in the city. However, Hermedia was not acting in his official capacity. He was acting as a paid agent of the US.

When Toscanino arrived, he was knocked unconscious, bound, blindfolded, thrown into the back seat of Hermedia's car, and driven to the Brazilian border. At the arrangement of the US government, he was then handed over to a group of Brazilians who held onto him for seventeen days. During this time, Toscanino alleges that he was constantly tortured and interrogated. Finally, on January 25, Toscanino was drugged and placed on a flight destined for New York, where he would stand trial.

This case strongly resembles tales of US efforts to bring terrorists to justice. But Toscanino was no terrorist. He was charged with conspiracy to import heroin into the US. This case is not a singular anomaly in drug trafficking prosecutions either.

The next year, one of Toscanino's co-conspirators Julio Juventino Lujan was targeted in another US capture operation. He was lured from Argentina to Bolivia by US agents using an intermediary. In Bolivia, Lujan was arrested by Bolivian police officers, "who were not acting at the direction of their own superiors or government, but as paid agents of the United States."[54] He was then brought to the airport, placed on a plane to New York, and taken into US custody upon landing.

Most famous of these capture operations was that of Humberto Álvarez Machaín in 1990. This Mexican doctor was accused of prolonging the life of a captured US Drug Enforcement Administration (DEA) agent. The doctor's actions allegedly facilitated the agent's torture and interrogation. To bring Álvarez Machaín to justice, the DEA hired Mexican policemen, civilians, and former military officers. All acting in their personal capacity, this group forcibly abducted the doctor from Mexico and flew him across the border to stand trial.[55]

Nevertheless, I learned that these cases are a relic of the past. They occurred during a time when drug traffickers in the most prolific host countries could live with virtual impunity. One such country was Colombia. Prior to 1991, the Colombian Constitution prohibited the extradition of its nationals. Therefore, pursuing countries had to rely on domestic prosecutions, which were fraught with issues. The US repeatedly struggled to have defendants brought before tribunals in Colombia that could be trusted. Judges were frequently paid off, threatened, or killed. In one instance, the US prepared several cases and sent prosecutors to work with their Colombian counterparts for a week to bring the drug traffickers to trial. These were slam dunk cases, yet one prosecutor lamented, "each case bounced with no conviction or a slap on the wrist."[56]

---

[54] *United States ex rel. Lujan v. Gengler*, 510 F.2d 62, 63 (1975).
[55] Sadoff, *Bringing International Fugitives to Justice*, 120.
[56] Prosecutor 10, interview.

Even the rare successful domestic prosecutions failed to satisfy US interests. They were never conducted in the open, so the public could not feel that justice was served. At the time, US prosecutors also believed that these defendants should be tried where the greatest harm was experienced. Simply put, prosecuting traffickers in Colombia did little to right the wrongs inflicted on the victims of drug epidemics in cities like New York.[57] These obstacles were unfortunately not limited to Colombia. Jodi Avergun, who was the Chief of Staff of the DEA and the nation's top drug trafficking prosecutor, explained that many heroin traders in the Golden Triangle of Southeast Asia were also protected from extradition and domestic prosecutions due to their threats to kill local officials.[58]

This all began to change in the 1990s. Countries began enacting legal reforms that enabled them to extradite drug traffickers. For instance, Colombia elected a new president who was committed to taking on the traffickers. His government subsequently amended their constitution to permit the extradition of nationals. As a result of this change, one prosecutor recalled that Colombia "went from 0 extraditions to our best extradition partner."[59] Jodi Avergun elaborated, "We didn't have to say, 'Okay, let's lure them or do something other than extradition' because the Colombian government, they have an extradition process and they would extradite.'"[60]

In addition, the US utilized foreign aid to encourage cooperation. In 2000, it enacted Plan Colombia, which provided funding to ten Latin American countries on the condition that they assist in rendering drug traffickers to the US. Jodi Avergun described to me just how effective this funding was in facilitating cooperation: "The US had total leverage in those kinds of cases … There was just like this [understanding], 'Hey, we …

[57] Prosecutor 10.
[58] Avergun, interview, September 25, 2020. Avergun served as Chief of USDOJ's Narcotics and Dangerous Drugs Section. She also previously served for twelve years as an Assistant US Attorney in the Eastern District of New York, including as the International Affairs and Extradition Coordinator.
[59] Interview with Prosecutor 10.
[60] Avergun, interview, August 21, 2019.

give you five billion dollars a year, give us who we tell you to give us.' Essentially that would happen with some minimal process."[61] The US adopted this same approach with those countries in the Golden Triangle, which similarly catalyzed cooperation.[62]

Likewise, host countries possess the political will to hand over drug traffickers. Similar to terrorism, they recognize this illegal conduct has damaging domestic impacts. So, they have an interest in bringing these individuals to justice. Jodi Avergun detailed:

> It was rare that a country sort of as a political statement would say we're not going to extradite on drug cases because for the most part, drugs are destructive wherever they are, not just where they're used but where they're grown. There are all sorts of incentives for corruption, money laundering, and violence. So, it's not like any country would say, 'It's a really good thing, we want it here … It's not our problem.'[63]

Along the same lines, drug trafficking cases have not experienced systemic challenges with state sponsorship. Jodi Avergun once again observed that "you didn't see governments involved in organized drug trafficking organization."[64]

The closest example to state sponsorship that she could recall related to Colombia's peace process. As part of the negotiations, the Colombian government made a political decision to block the extradition of drug traffickers involved in that country's internal armed conflict. However, Avergun was quick to differentiate this from the type of state sponsorship seen in cybercrime: "Russia … doesn't want us to have their hackers because their hackers are working for the government. Here, this was Colombia wanting us to forgo extradition because they would have the end of a civil war."[65] Therefore, the US was content to drop its extradition claims in order to help end the hostilities.

Although it was not an internationally recognized state, another example would be Afghanistan while under the control of the Taliban. This terrorist organization used opium

[61] Avergun.
[62] Avergun, interview, September 25, 2020.
[63] Avergun, interview, August 21, 2019.
[64] Avergun.
[65] Avergun.

trafficking to finance its activities, selling between 2,000 and 9,000 metric tons a year.[66] However, Jodi Avergun explained that these cases were generally handled as a counterterrorism matter with law enforcement, such as the DEA, only providing support and intelligence. In fact, only two drug traffickers tied to the Taliban have been brought to justice in the US. One was lured to the US in 2005 during the reconstruction period, and another was extradited by Afghanistan in 2009.[67] It's important to note that, as Jodi Avergun emphasized, these cases and the Taliban's role as a narco-state were truly "*sui generis*" occurrences in the realm of drug trafficking.[68]

The challenges in bringing drug traffickers to justice generally stemmed more from corruption rather than a state actively sponsoring or seeking to protect these offenders. Corrupt officials could bury evidence, alert drug traffickers of arrest attempts, or tank extradition proceedings. This is particularly problematic considering that drug trafficking often occurs in countries with high incidences of poverty. These crimes generate substantial illicit proceeds, providing a steady stream of money for pay-offs.

The menace of corruption was on full display in the prosecution of Joaquin "El Chapo" Guzman. As leader of the Sinaloa drug cartel, Guzman imported tens of thousands of kilograms of narcotics into the US. In 2017, he was finally extradited to New York. At trial, details emerged regarding corruption that reached nearly every level of the Mexican government: prison guards, airport officials, police officers, prosecutors, tax assessors, and military personnel.[69] These compromised officials would alert Guzman of any attempts to arrest him, providing an opportunity to flee and preventing his extradition. In one

[66] Dwyer, "The U.S. Quietly Released Afghanistan's 'Biggest Drug Kingpin' From Prison. Did He Cut a Deal?"
[67] Weiser, "Afghan Linked to Taliban Sentenced to Life in Drug Trafficking Case"; "Haji Bagcho Sentenced to Life in Prison on Drug Trafficking and Narco-Terrorism Charges."
[68] Avergun, interview, September 25, 2020.
[69] Feuer, "El Chapo Trial Shows That Mexico's Corruption Is Even Worse than You Think."

astounding revelation, witnesses testified that Guzman paid a $100 million dollar bribe to the former President of Mexico in return for ending a nationwide manhunt.[70]

Nevertheless, the US has still relied on host countries for cooperation despite the challenges of corruption. In other words, the US has not generally resorted to unilateralism. After all, the El Chapo case was ultimately resolved through a successful extradition from Mexico. As Jodi Avergun recollected to me:

> The DEA was very good at creating vetted units within a lot of the national police forces and countries where drugs were a particular problem. And if you had a vetted unit, which meant that they were polygraphed and extensively background checked before they were allowed to work on this kind of task force, then you didn't necessarily need to go through a process to get them out of the country outside the knowledge of a law enforcement entity in that country.[71]

The US would often fund the creation of such vetted units. The first was implemented in Mexico, where corruption was rampant, and experienced considerable success, leading to the replication of this model in other countries of concern.[72]

Even when corruption poses a barrier, I learned that drug trafficking cases still face less of a need for unilateralism. Drug traffickers, particularly kingpins, tend to travel on their own. As their business expands, they seek to enlarge their networks. Different parts of the production cycle are generally located in different countries. Cocaine and heroin may be grown in Colombia, but the logistics and importation to the US are usually handled in Mexico. So, as drug trafficking organizations grow and become vertically integrated, the higher-level leaders must often meet in-person to build trust as prospective partners.

Such cross-border travel then enables these kingpins to be tracked to third countries, where they may not be able to buy the protection of government officials.[73] Once located, these cases can proceed through extradition, quasi-extradition, or self-

[70] Fernandez and Ferman, "El Chapo Highlighted Mexican Corruption, but Drug Money Also Lubricates U.S. Border."
[71] Avergun, interview, August 21, 2019.
[72] Avergun, interview, September 25, 2020.
[73] Avergun, interview, August 21, 2019.

surrenders. In other words, drug traffickers essentially lure themselves through their travel habits, creating less of a need for unilateral action.

In fact, one prosecutor explained how self-surrenders are more common in the drug arena than for other transnational crimes due to public safety reasons. Law enforcement recognizes that drug traffickers are generally dangerous individuals. A self-surrender can therefore avoid their arrest devolving into a violent altercation that would pose a risk to the lives of law enforcement and bystanders.[74]

Drug trafficking cases also face a diminished need for unilateral alternatives relative to cybercrime since there is no significant attribution challenge. Drug traffickers strive to maintain their anonymity. However, their crimes typically leave traceable physical evidence. They must also interact with other members of the conspiracy who learn their identity and can be turned into criminal informants. As Jodi Avergun remarked, "none of [this] is true for cybercriminals."[75] Consequently, drug traffickers "have these powerful ways of keeping them[selves] from being found, but they are findable."[76]

Moreover, drug traffickers pose less of an imminent threat than cybercriminals. This mitigates against using unconventional tools, such as unilateral alternatives. There is simply less of a rush to secure custody. While imported narcotics will undoubtedly cause harm in the victim country, it is unlikely than anyone will be gravely hurt or killed in transit. This reduces the need for swift action.[77] Plus, as Jodi Avergun lamented, arresting a member of a drug trafficking organization, even a kingpin, does little to stop the flow of drugs. There is always another person in line, ready to fill the kingpin's shoes in case he is

[74] Prosecutor 7, interview.
[75] Avergun, interview, August 21, 2019.
[76] Prosecutor 7, interview.
[77] Prosecutor 48, interview.

arrested.[78] This is precisely why the Sinaloa cartel has continued to pump illegal drugs into the US despite El Chapo's arrest.

Prosecutors thus have the flexibility to wait for a formal extradition to proceed or for the defendant to travel to a jurisdiction from which he can be rendered. Jodi Avergun captured these sentiments by explaining, "I don't remember it ever really factoring in, like having a case where 'Oh my gosh, we have to get this person out…'"[79]

As a result of all these factors, I find that drug trafficking prosecutions simply face less of need for unilateral capture or lure operations. In fact, Álvarez Machaín was the last non-terrorist to be rendered via a capture operation.[80] Since that case, capture operations have been "reserved for the counterterrorism context and not law enforcement. It's mostly intelligence agencies that do it."[81] While prosecutors might be hesitant to acknowledge the more recent use of a capture operation, such a case would draw significant media attention. However, a review of news databases uncovered no such cases, supporting the reliability of these observations.

Even if there was a need for unilateralism, prosecutors highlighted that lure operations are less viable here. There are certain rules of engagement that govern the types of actions in which US officials can engage unilaterally within a foreign country. Face-to-face contact still pervades interactions between drug traffickers, which can significantly constrain the ability for law enforcement to devise a lure operation.[82] If an undercover agent cannot build trust with a target on the ground in the host country, he is unlikely to convince the trafficker to travel on a ruse.

[78] Avergun, interview, September 25, 2020.
[79] Avergun, interview, August 21, 2019.
[80] Prosecutor 44, interview.
[81] Avergun, interview, August 21, 2019.
[82] Avergun, interview, September 25, 2020.

Is cybercrime apt to follow the same transformation as drug trafficking from unilateralism to a reliance on international cooperation? One of the most important catalysts of this change in drug trafficking was legal reform in the most prolific host states. Indeed, the most prolific host states in cybercrime have similar legal provisions barring the extradition of their nationals.

However, a viable alternative exists now: host countries could domestically prosecute their cybercriminals. In drug trafficking, host countries attempted such domestic prosecutions, but these failed due to weak judicial systems. In cybercrime, the most prolific host countries make no effort to domestically prosecute offenders. This failure cannot be attributed to a lack of capacity. These countries know very well how to prosecute cybercriminals that target their own citizens and institutions. For instance, in 2012, Russian police successfully arrested and prosecuted eight cybercriminals who stole $4 million from over 100 banks and businesses around the world, including in Russia.[83]

Rather, as seen in Chapter 4, these countries simply choose not to prosecute since it is not in their interests. This indicates that cybercrime host countries are not likely to implement the legal reforms to permit the extradition of their citizens. Even if they were to make such changes, these countries, particularly state sponsors, would likely find ways to not comply and continue providing safe haven. Indeed, we have seen examples of how some of the US's strongest extradition partners, such as the United Kingdom, have found pretexts to deny extradition for cybercrime when doing so was in their political interests.

One of the factors that facilitated legal reform was drug traffickers turning against their home countries, thus creating a domestic imperative to bring these individuals to justice. Can we expect to see a similar transformation in cybercrime that would change the perspective of the most prolific host countries? While such a change is possible, it does not

[83] Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals."

appear likely. Cybercriminals already have a vast victim pool abroad and can target these individuals without affecting their homeland. So, they have little incentive to change course. In fact, existing academic research has repeatedly documented a tacit understanding in Russian cybercriminal communities to not target their fellow citizens. The malware used by Russian and Eastern European cybercriminals is even crafted to avoid affecting computers in the perpetrators' home countries.[84]

For those rogue cybercriminals who breach this understanding, their home countries have already made clear the consequences of such actions. As one cybersecurity industry report documented, "hackers that engage in malicious activity in post-Soviet countries are arrested on a regular basis."[85] In the 2012 Russian prosecution cited above, the police sought to make an example out of those cybercriminals. They released to the media a video of one of the defendants loudly weeping after his home was raided.[86]

Even if increased competition and improved cyber defenses abroad cause cybercriminals to turn against their compatriots and generate local public backlash, the most prolific host countries can deal with these offenders on their own. Both China and Russia have internet security laws that facilitate the surveillance and evidence gathering necessary to attribute cyberattacks and prosecute the perpetrators. For example, "with specialized hardware and software installed in every Russian internet service provider, governmental and law enforcement agencies now have on-demand access to the private data of Russian citizens without the need to provide a court order."[87] Consequently, these countries would have little reason to cooperate with the US. They can single-handedly

[84] Maurer.
[85] Yakovlev, "The Dark Side of Russia: How New Internet Laws and Nationalism Fuel Russian Cybercrime," 7.
[86] Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals."
[87] Yakovlev, "The Dark Side of Russia: How New Internet Laws and Nationalism Fuel Russian Cybercrime," 4.

bring to justice those cybercriminals causing harmful domestic effects while allowing cybercriminals who target other countries to run rampant.

One evolution that occurred in drug trafficking and could change the perspective of certain host countries is if cybercrime turns violent and increasingly threatens human health and safety. For those countries that lack the political will to assist, the gravity of these harms may demonstrate to them that cybercrime is a serious offense and that the perpetrators cannot be allowed to live with impunity. However, even these significant potential harms may not be enough to convince state sponsors to cooperate.

During the COVID-19 pandemic, Russian cybercriminals have launched ransomware attacks against hospitals and the health care sector. Such attacks can have dire consequences by taking key medical systems offline, delaying urgently needed treatments or the release of important test results. Cybersecurity expert Michael Holden, who has been tracking these attacks, has "no doubt that the Russian government is aware of this operation."[88] Yet, the Russian government has taken no meaningful enforcement action. This suggests that even as the cyber threat increases in severity, state sponsors will continue to provide safe haven as long as the offenders do not target domestic victims.

Could the US then turn to foreign aid to encourage cooperation in the same way that it did for drug trafficking? The difficulty here is that cybercrime brings significant value to host countries. It injects illicit proceeds into their economy. In Russia alone, the cybercrime market is estimated to be $2.3 billion.[89] And, coopted hackers enable them to project power and achieve foreign policy objectives.

At the same time, these actions have little to no domestic costs since cybercriminals know not to target domestic victims. This cost-benefit analysis for host

[88] Bajak, "FBI Warns Ransomware Assault Threatens US Healthcare System."
[89] Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals."

countries stands in stark contrast to that for drug trafficking, which generated significant costs for host countries in terms of corruption, drug use, and violence. While corruption is still a concern for cybercrime, the overall benefits to host countries are likely to dwarf these costs and any possible foreign aid the US could provide, limiting its effectiveness.

Foreign aid would likewise be politically infeasible considering which host countries are the most pernicious for cybercrime. The US could not provide millions to hostile countries like China, Iran, North Korea, and Russia without generating significant public backlash. Additionally, such aid may run counter to other US foreign policy goals with these countries by essentially rewarding rogue behavior. It could remove the incentives for these countries to reform other aspects of their policies, such as on human rights, international trade, or nuclear nonproliferation.

Unlike drug trafficking, cybercrime prosecutions also cannot simply wait for perpetrators to travel to third countries. As we learned in Chapter 4, cybercriminals do not generally travel for business reasons. Even if they do travel, their extradition is not guaranteed since their home country may interfere in the process.

None of the changes seen in drug trafficking can address the attribution challenge in cybercrime either. Rather, given their tacit support or sponsorship of cybercrime, host countries will likely continue to refuse cooperation in these investigations, denying law enforcement the critical evidence needed to "put the butt in the seat." So, cybercrime cases will continue to require unilateral lures to overcome this difficulty in establishing identity.

Plus, cybercrimes are happening in real time with devastating financial impacts on victims. This necessitates a more urgent response to stem the bleeding, which can be accomplished by arresting the perpetrators. Unlike drug trafficking where the kingpins can easily be replaced, removing the individuals with the technical expertise to commit

cyberattacks can have a meaningful impact in ending the conduct. Hence, there is a greater urgency to secure custody over the offender.

Considering the lack of more cooperative remedies, lures may be the only way to achieve this outcome. And they are viable here. Since cybercrime takes place online, lures almost entirely take place online and do not require undercover law enforcement agents to enter the host country. So, the rules of engagement, which can hamstring such operations in drug trafficking cases, would not constrain cyber prosecutions.[90]

5.3 Fraud and Foreign Corruption: Limited Need for Unilateralism

Newspapers may not be emblazoned with headlines of sensational attempts to bring perpetrators of transnational fraud to justice. Nor are commandos likely to unilaterally capture those participating in foreign corruption. However, as the world economy becomes increasingly interconnected, this area of transnational criminality has been an area of growing law enforcement interest. It is also an area that could rely on less extreme unilateral alternatives, namely lure operations.

Yet, as this section lays out, I learned that these prosecutions have not needed to rely on unilateralism due to the profile of the offenders and nature of the conduct. The defendants often reside in cooperative countries, are willing to waive extradition, or can be arrested and extradited while traveling to conduct business. A unilateral response is also less feasible since it can introduce unnecessary risks at trial. After all, prosecutors can still have a deterrent effect by simply unsealing the indictment or charging the corporation.

Alternatively, cybercriminals have every incentive to fight against extradition and no business reason to travel to countries that will assist in handing them over. At the same time, there is a greater need to secure physical custody since unsealing an indictment or

[90] Avergun, interview, September 25, 2020.

charging a criminal entity has less deterrent effect. This means that unilateral alternatives may be a necessary risk to bring these perpetrators to justice.

Transnational fraud refers to a broad portfolio of international financial crimes. These include accounting fraud, commodities fraud, corporate fraud, financial institution fraud, market manipulation, insider trading, investment fraud, and telemarketing fraud.

It is important to differentiate this category of offenses from cyber-enabled frauds where the use of computers or other information technology is central to the crime and are considered cybercrimes. Examples of cyber-enabled frauds include certain advance fee frauds, scam emails, and business email compromise. The integral role of technology here means that these offenses can be conducted entirely remotely, perpetrators can hide from identification behind the anonymity of the internet, and depending on the type of conduct, the host country may wish to protect the offenders or even sponsor the activity. These characteristics, which all alter the prospects for securing custody over the perpetrator, are shared with cyber intrusions and attacks. Therefore, for the purposes of this analysis, they are deemed cybercrimes and evaluated together.

Despite fraud perpetrators being located abroad, the prosecutors I interviewed indicated that securing custody tends to proceed without major challenges. I learned that fraud defendants are more likely to waive extradition.[91] One prosecutor explained that these international businessmen are accustomed to freely crossing borders. However, an extradition request or Red Notice can significantly impede their ability to do so. So, many would rather come to the US and address the pending criminal charges than live trapped in their country of residence as extradition proceedings drag on for years. Given the profile of these defendants as international businessmen, many decide to cooperate in order to avoid

[91] Prosecutor 15, interview.

sitting in a US prison.[92] Flipping on their co-conspirators thus minimizes the downside of waiving extradition.

Indeed, certain fraud defendants may not care if their ability to travel internationally is constrained. For example, one prosecutor reflected that telemarketing fraudsters generally do not travel outside their home countries. So, their incentives to waive extradition may be minimized. However, the prosecutor noted that the US has still been able to lay hands on these defendants. In fact, the countries where fraud defendants are located usually tend to cooperate through extraditions. Many international fraudsters sought by the US are located in Europe and South America, which are hubs for international business and finance. As a result, one prosecutor explained to me that there have been "no real examples of gamesmanship" that would block extradition.[93]

Additionally, fraud defendants are less likely to be seen as the "kid next door" and thus deserving of public sympathy. In fact, there are generally negative public attitudes toward business executives, particularly those in the finance sector. For instance, a YouGov-Cambridge poll found that 83% of UK adults believed that bankers are greedy and are excessively compensated. 58% also believed that "bankers are at best unprofessional, and at worst dishonest."[94] This scenario contrasts with the Gary McKinnon and Lauri Love cybercrime cases, where public sympathy generated sufficient backlash for the UK to take a stand against extradition. Rather, there is not likely to be significant public outcry against handing over a business executive, eliminating a potential political challenge here.

Recently, the Forum Bar has complicated the US-UK extradition relationship. In 2013, the UK amended its Extradition Act of 2003 to permit judges to deny extradition

[92] Prosecutor 61, interview, October 1, 2020.
[93] Prosecutor 61.
[94] "Public Trust in Banking."

when the offense could be feasibly and timely prosecuted in the UK and/or it would not be in the interest of justice to extradite. The latter occurs when a substantial amount of the crime took place in the UK and the defendant has significant connections to the UK.

Since its enactment in 2013, "all attempts to use it as a bar to extradition failed, leading many practitioners to believe that it was a bar in name only."[95] However, for transnational fraud, this all changed in 2018. The US had accused British national Stuart Scott of participating in fraudulent foreign exchange trading. His employer, HSBC, won a bid to convert $3.5 billion USD into pound sterling for the Scottish company Cairn Energy. As part of this deal, HSBC was required to act in Cairn's best interests. Yet, the US alleged that Scott and a fellow trader used their insider knowledge to artificially raise the Pound/Dollar price in advance of the trade, reaping in cash for HSBC to the detriment of Cairn. The US also claimed that Scott and his fellow trader maliciously advised Cairn that it was best to execute the trade at the exact moment when the market was easiest for them to manipulate.[96]

Scott challenged his extradition under the Forum Bar and appealed the case to the High Court of England and Wales. The Court ultimately ruled in his favor for two main reasons. First, the only quantifiable harm occurred to Cairn, a British company. Thus, the harm occurred in the UK, not the US. Second, Scott had significant connections to the UK. He was a citizen, lifelong resident, and facing substantial pressures due to the illnesses of family members in Britain. Consequently, extradition was denied. This occurred even though the UK Serious Fraud Office publicly declared it had insufficient evidence to convict in the UK, taking domestic prosecution off the table.[97]

[95] "Forum Bar - Finally in Force?"
[96] Saugman, "UK Courts Raise the Bar to US Extradition."
[97] Saugman.

This case reveals that the US may face increasing difficulty bringing UK fraud defendants to justice. Not only may their extradition be denied but they may also escape punishment in their home country. However, one prosecutor explained to me that USDOJ has significantly improved its intake procedures to weed through cases. This ensures the US is only focusing law enforcement resources on those crimes that present a compelling federal interest.[98] Such cases would then avoid running afoul of the forum bar. They would demonstrate that a substantial degree of harm occurred in the US, undermining arguments against extradition like those Scott raised.

In addition to the cooperativeness of the most important host countries, there are fewer legal barriers to extradition for fraud cases. Given that fraud is such a basic offense, most countries have relevant statutes that satisfy dual criminality. However, US prosecutors have encountered some legal difficulties when they have charged individuals with conspiracy to commit fraud. Certain countries do not have equivalent laws for conspiracy, even if the underlying crime is criminalized.[99] One prosecutor also explained that the US can sometimes "push the envelope" on the definition of fraud and theory of liability in the case.[100] Depending on the interpretation of the judge in the host country, this could create a dual criminality barrier.

Nevertheless, prosecutors can adjust their indictment strategy to ensure at least some common offenses are charged to create the grounds for extradition. They can also work to convince the host country that the underlying conduct criminalized by both countries' laws is sufficiently similar to satisfy dual criminality. And if none of these approaches succeed, they can typically wait for the defendant to travel to a country without such legal barriers. These defendants are businessmen who live international lifestyles and

[98] Prosecutor 61, interview, October 1, 2020.
[99] Prosecutor 32, interview.
[100] Prosecutor 61, interview, October 1, 2020.

travel for work. As one prosecutor observed, "the nature of these offenses is a panacea for us. Business crimes require business to be done, which often means talking to people and traveling."[101] Thus, a wait and see approach is a viable possibility.

Even if all the above potential solutions fail, unilateral action would not likely be pursued. The prosecutors I interviewed repeatedly asserted that lures are generally avoided from rule of law countries or countries that are strong law enforcement partners.[102] These are often the same countries where transnational fraudsters are based, so a lure would be less favored. One prosecutor relayed to me, "Let's just say there's a friendly country where we don't have dual criminality. Would we do a unilateral lure? We'd think carefully about it because you could really compromise our relationships with law enforcement agencies."[103]

Plus, lure operations risk undermining the prosecution's case here. One prosecutor explained to me that in a fraud trial, the government is alleging that the defendant engaged in some type of material deception. Yet, committing a material deception is precisely what law enforcement is doing in a lure. Consequently, prosecutors fear that if a defendant were to raise details of the lure at trial, it would make the government look hypocritical and potentially turn the jury against them. Considering that fraud defendants usually can be extradited or travel, this risk of a lure simply does not justify the possible benefits, in the prosecutor's view.[104]

Even if such an offender cannot be extradited or does not travel, law enforcement still has another, less risky arrow in its quiver. Typically, prosecutors charge these perpetrators under seal to protect witnesses, preserve evidence and the integrity of the investigation, and prevent the fraudster from fleeing. However, once all the goals of

[101] Prosecutor 61.
[102] Prosecutor 17, interview; Prosecutor 20, interview; Prosecutor 23, interview.
[103] Prosecutor 17, interview.
[104] Prosecutor 61, interview, October 1, 2020.

sealing are satisfied, prosecutors may move to unseal the charges. As one prosecutor explained to me, there is a significant degree of public shaming associated with an unsealed USDOJ indictment, which serves a specific and general deterrent purpose, among others. Corporations may not want to employ such a perpetrator as an executive under these circumstances. This significantly reduces the executive's ability to earn a livelihood in the form and to the extent previously enjoyed. And it may put an end to certain of his misconduct by restricting access to the market institutions frequently necessary to commit financial fraud.[105] This means that law enforcement could effectively disrupt or prevent future crimes without resorting to a lure.

In fact, unilateral lure operations are also less feasible for many fraud cases. Approximately half of these investigations are overt, retrospective, and long running. For example, they may begin as the prosecution of a corporation that law enforcement then convinces to cooperate against the executives involved. As a result, the individual defendants will generally know that they are under scrutiny. So, if they are seeking to evade capture, they will be careful not to travel to countries from which they could be extradited and less likely to fall for a lure.[106]

As an example, one prosecutor pointed to the case against Volkswagen Group, its CEO Martin Winterkorn, and five other Volkswagen employees and executives. Volkswagen had begun a massive push to sell diesel cars in the US. This included popular models such as the Jetta, Beetle, Golf, and Passat. At first glance, these cars appeared to run fine. They all passed nitrogen oxide emissions tests. But, there was a catch. Volkswagen had installed a defeat device on these cars that would activate emissions controls on nitrous oxide. These emissions controls would only kick in when the vehicles

[105] Prosecutor 61, interview, December 3, 2020.
[106] Prosecutor 15, interview.

were undergoing testing, deceiving the US Environmental Protection Agency. When the cars were driven on the road, the nitrous oxide emissions exceeded 40 times the legal limits in the US.[107]

All six defendants are German citizens and reside in Germany, whose constitution prohibits the extradition of its nationals. Hence, this case could present the need for a lure. However, like many fraud cases, US law enforcement had been in contact with Volkswagen, which was charged as a corporation and reached a plea agreement in 2017. By the time an indictment was filed against Winterkorn and the other executives in 2018, they knew their company's actions were under criminal scrutiny. They knew to be cautious with their international travel to avoid arrest, which would foil a lure attempt.[108]

Foreign corruption presents a similar outlook for securing custody. The US Foreign Corrupt Practices Act (FCPA) makes it illegal for American corporations and their employees and officers to bribe foreign officials. These bribes could be to influence the officials in their government duties, induce them to violate their duties, or gain any improper advantage. Since its passage, the scope of FCPA has been expanded to include foreign firms that attempt to commit bribery in the US. It also now covers any company whose securities are listed on a US exchange.[109]

Similar to fraud cases, prosecutors reported less of a need for unilateral tools in foreign corruption cases. US District Court Judge Trevor McFadden previously championed USDOJ's foreign corruption enforcement as the Principal Deputy Assistant Attorney General of the Department's Criminal Division.[110] He explained to me that foreign corruption cases originally focused on corporate criminal liability with very few

[107] Hotten, "Volkswagen: The Scandal Explained."
[108] Prosecutor 15, interview.
[109] "Foreign Corrupt Practices Act."
[110] Judge McFadden also previously served as an Assistant US Attorney in the District of Columbia and litigated FCPA matters while at the firm of Baker & McKenzie.

standalone cases against individuals.[111] So, securing physical custody was less of a pressing concern. This decreased the likelihood that law enforcement would turn to such extraordinary measures like a unilateral alternative.

Over time, FCPA resolutions against companies have increasingly been accompanied by prosecutions of individuals.[112] However, these cases tend to focus on senior executives who live international lifestyles. The defendants "travel all the time as a function of their jobs, so we can often catch them while an indictment is still under seal."[113] Prosecutors reported that the criminal conspiracy frequently requires these perpetrators to travel since they must talk and have face-to-face meetings to pay bribes. As a result, the US has been able to issue Interpol Red Notices and wait for them to travel to any number of locations from where they can be extradited.[114] Similar to fraud defendants, their status as international businessmen also means that these perpetrators do not wish to have international arrest warrants or Red Notices outstanding. Consequently, they are more likely to voluntarily surrender or waive extradition.[115]

Nevertheless, Judge McFadden recalled that "extradition is not always a slam dunk" for these cases.[116] FCPA can be controversial, even in countries with which the US maintains strong law enforcement partnerships. This law provides uniquely extraterritorial jurisdiction to the US.[117] Therefore, countries may view US enforcement attempts, particularly when neither the bribe payor nor payee are US citizens, as intruding on their sovereignty. In these scenarios, the degree of harm and nexus to the US may appear tenuous. Rather, the host country may believe it is solely their responsibility to prosecute

[111] McFadden, interview.
[112] McFadden.
[113] Prosecutor 61, interview, October 1, 2020.
[114] Prosecutor 61.
[115] McFadden, interview.
[116] McFadden.
[117] McFadden.

since the conduct involves their citizens, businesses, and/or government officials. Such host countries may then be less willing to assist on an extradition request.

However, Judge McFadden observed that these challenges are becoming easier to overcome due to the UN Convention Against Corruption, which has near universal approval. This legally binding international treaty mandates parties to take certain preventive measures against corruption, criminalize specific conduct, cooperate in international investigations through mutual legal assistance and extradition, institute asset recovery procedures, and participate in technical assistance and information sharing programs. To date, there are 186 parties to the Convention, and only six countries have neither signed nor ratified it.[118]

Owing to the Convention, Judge McFadden commented that there is "greater recognition that this a global issue, which has empowered the US," particularly related to extraditions.[119] Moreover, the US has improved its intake of cases to ensure there is a compelling US interest in prosecution. At the intake stage, the US also engages in informal negotiations with the other involved countries to iron out who has equities in pursuing the case.[120] As a result, those countries that would object to US jurisdiction can instead prosecute the case domestically. The charged corruption would usually be outlawed under their laws, so they can bring these individuals to justice in their courts. Consequently, Judge McFadden affirmed that "no FCPA safe havens immediately spring to mind."[121]

The one potential exception he highlighted was China. There, the government may place pressure on companies not to cooperate with US investigations. This may not only block extraditions but also make it difficult to identify the culpable individuals. Nevertheless, Judge McFadden noted that this is less of a concern for companies that

[118] "United Nations Convention Against Corruption."
[119] McFadden, interview.
[120] Prosecutor 61, interview, October 1, 2020.
[121] McFadden, interview.

operate around the world.[122] Requests for information or mutual legal assistance can be conveyed through more cooperative countries where the corporations also operate. Culpable individuals can be apprehended while travelling internationally. And these businesses may feel compelled to cooperate with investigations to avoid being shut out of global markets. Therefore, these challenges do not reach the same level of state sponsorship seen in cybercrime nor generate the same need for unilateral alternatives.

Can any lessons be extrapolated from fraud and foreign corruption cases to cybercrime? As previously noted, cybercriminals face no need to travel. This precludes the "wait and see" approach or hoping that they will simply waive extradition. Cybercriminals are not international businessmen who have any professional reason to cross borders. They can engage in incredibly lucrative criminal conduct from the comforts of their homes in safe haven countries. As a result, the presence of an international arrest warrant or Red Notice poses no real threat to their way of life in the manner it does for an international business executive. This means they will be less inclined to self-surrender.

The incentives for cybercriminals to turn themselves in are further diminished by the fact that they can often successfully contest their extradition. As one federal agent reflected to me, "there is nothing they won't try to muddy up the waters or challenge the government on" with respect to extradition.[123] Another federal agent agreed that cybercriminals "will fight tooth and nail if they are fighting extradition."[124]

This is because the three main questions that the extraditing county's courts typically consider are whether the death penalty is a possibility, dual criminality is satisfied, and the requesting government can prove they have identified the correct perpetrator. Given the persistent challenges of attribution, cybercriminals can easily

[122] McFadden.
[123] Federal Agent 12, interview, September 15, 2020.
[124] Federal Agent 11, interview, September 16, 2020.

contest extradition on those grounds.[125] This tends to be less of a concern in fraud and corruption cases since law enforcement often has informants or the charged company may be cooperating against the executives involved. Thus, fraud or corruption defendants would have less of a viable basis to challenge their extradition.

In fact, considering the role of state sponsorship, the scales may be more frequently tipped in cybercriminals' favor. Their home country can seek to interfere in the extradition process and protect them. For instance, when Russian cybercriminals are arrested abroad, "the highest levels of [the Russian] government support the claim that the person is wrongfully accused and an upstanding citizen."[126]

This contrasts with fraud and foreign corruption cases where a prosecutor I interviewed could not recall a single instance of extradition interference.[127] Yet, as we saw in Chapter 4, such attempts have succeeded in multiple cybercrime cases, allowing the perpetrator to escape justice. Therefore, if a cybercriminal knows his home country may come to their rescue, he would have less of a reason to waive extradition.

In further contrast to fraud and corruption cases, cybercrime defendants may also face significant potential sentences for their conduct. They know that they cannot bribe their way out of jail in the US. So, they may elect to challenge their extradition rather than risk a lengthy US prison sentence.[128] In the MegaUpload case discussed in Chapter 4, Kim Dotcom was facing a potential sentence of up to 20 years in prison. Yet, the New Zealand courts released on him bail merely a month after he was arrested. They also provided him with access to the illicit funds he had earned to cover his legal fees and living expenses. As a result, Dotcom had every incentive to launch multiple appeals and fight extradition.

[125] Federal Agent 12, interview, September 15, 2020.
[126] Federal Agent 12.
[127] Prosecutor 61, interview, October 1, 2020.
[128] Federal Agent 12, interview, September 15, 2020.

Now, eight years after his arrest, he still has not been rendered to the US.[129] In fraud and corruption cases, the sentences are much lower, so the risk of waiving extradition and standing trial in the US is less of a concern. Fraud and corruption defendants also recognize that they can mitigate the punishment by cooperating with US authorities.

Moreover, there is a greater need to secure physical custody over perpetrators of cybercrime than in fraud and corruption cases. The priority is on arresting the individual rather than charging a corporation. Cybercriminals do not seek to run legitimate businesses, so their operations would not be negatively impacted by a corporate criminal prosecution in the same way. In addition, while some cybercriminals have become increasingly organized, their operations may still be too loose to be considered a chargeable corporate entity.

For those cybercrime businesses that could be indicted, such enforcement action will likely only have a short-term impact. A new, more covert replacement will likely soon pop up in its place, which occurred after the takedowns of the Silk Road dark web marketplace and prominent cybercriminal forums.[130] To have a real deterrent effect, law enforcement will need to bring the individuals behind these enterprises to justice in order to end their illicit conduct for good and prevent them from starting anew.

For this same reason, law enforcement cannot rely on simply unsealing an indictment against cybercriminals. While this may reveal their *modus operandi* and help potential victims harden their defenses, the perpetrators can simply change their method of attack. There are also less concerns about cybercriminals being outed. They typically operate using nicknames, so they could simply reinvent themselves online and continue victimizing further individuals and organizations. Thus, when extradition fails, pursuing

[129] Sinclair, interview.
[130] Farivar, "After Silk Road Takedowns, Dark Web Drug Sites Still Thriving"; "Forums Are Forever – Part 1: Cybercrime Never Dies."

countries will still need to secure custody, such as through unilateral alternatives. Plus, unsealing an indictment is only effective if law enforcement has identified the perpetrator, which is often not possible in cybercrime cases without the help of a lure operation.

Additionally, fraud and foreign corruption cases enjoy greater international consensus, which is not likely to occur for cybercrime. Given the support of cybercrime by the most prolific host countries, law enforcement cannot rely on these countries to extradite or prosecute offenders. There is also not the same global normative pressure for cooperation in cybercrime. While the UN Convention on Corruption has reached near universal acceptance, the most prolific host countries seek to undermine consensus on cybercrime. They seek to sow discord in the international community and forestall the expansion of the Budapest Convention by drafting their own, weaker cybercrime treaty. This concerted effort indicates that the lack of consensus is not merely an instance of regulatory lag that will improve over time. Rather, it is a persistent political component of cybercrime, which will continue to leave pursuing countries with a need for unilateralism.

In fact, a unilateral response is more viable in cybercrime. Such investigations are generally covert, allowing a lure to succeed since the offender is unaware that they are under scrutiny. There is also less of a concern that the use of a lure could backfire with the jury in a cybercrime case. Many of these prosecutions focus on computer intrusions and the pilfering of data, such as payment card information. So, the theory of liability centers more on a trespass or theft than a fraudulent deception.

Nine of the twelve known cybercrime cases involving a lure were hacking prosecutions. The language used by law enforcement in these cases is more evocative of a trespass or theft, further suggesting that the theory of liability centered less on a material deception. For instance, the terms “unauthorized access,” “breaking into,” “extortion,” “illegally entered,” “bank robbery for the virtual age,” and “virtual theft” all featured

prominently in press releases and sentencing documents. Another one of the twelve known cybercrime cases involving a lure operation was an "online piracy" prosecution, which is more akin to a criminal copyright violation than a material deception and fraud.

Indeed, there are certain cyber-enabled frauds where the theory of liability is based on a material deception. However, due to the inherent evidentiary and political challenges of cybercrime outlined in Chapter 4, law enforcement may have no viable alternative to secure custody. Unlike a fraud case, they may not be able to rely on an extradition or wait for the defendant to travel. Thus, the benefits of bringing the cybercriminal to justice through a lure operation may outweigh the risks.

5.4 Export Controls and Sanctions: Shared Political Challenges to Cybercrime

Perpetrators residing in safe havens, state sponsorship, and extradition interference. This description could refer to the political challenges laid out in Chapter 4 of securing custody over international cybercriminals. Yet, as this section details, I learned it just as easily characterizes export control and sanctions cases. This has led to a sustained reliance on unilateral alternatives in the form of lure operations to bring violators to justice.

These findings foreshadow that a similar sustained reliance may occur for cybercrime. Indeed, the need may be even higher in cybercrime due to the attribution challenge and remote nature of these offenses, which means perpetrators do not have to travel as part of the conspiracy. Plus, cybercrime is inherently a criminal justice matter with tangible victims. So, there is a greater need to arrest the perpetrators and stop the ongoing losses for those victims.

Export controls refer to the restrictions that countries place on the international sale of certain merchandise. The goal: to protect national security, foreign policy, or economic interests. These items typically require a specific license from the government to be sold abroad since they have a dual use. They can be employed for both civilian and military

applications. This raises concerns that the technology could fall into the hands of foreign adversaries or hostile nonstate actors.

The export control regime is closely related to trade sanctions, which prohibit the persons and entities of a given country from engaging in economic activity with specified other countries. The goal here is to place diplomatic pressure and an economic squeeze on the targeted country in order to change their behavior in some way.

Similar to cybercrime, I discovered that one of the greatest challenges of bringing violators of export controls and sanctions to justice is their location. They typically reside in uncooperative jurisdictions: the very countries targeted by these restrictions. These countries already have hostile or strained relations with the pursuing country and are therefore not likely to assist. Jay Bratt, who oversees the nationwide prosecution of these offenses as Chief of USDOJ's Counterintelligence and Export Control Section, estimated that 40% of cases involve Iran, 25% involve China, and 15% relate to North Korea, Pakistan, and Syria. Thus, he approximated that at least 80% of these defendants are based in jurisdictions that would not extradite or informally cooperate in handing them over.[131]

This lack of cooperation is not only due to the strained diplomatic relationship. It is also due to the host countries' vested interest in protecting export control and sanctions defendants, creating a predicament of state sponsorship. The perpetrators assist these countries in gaining access to superior technologies and commodities developed abroad. This in turn fuels their technological and economic growth and helps narrow the gap in military capabilities by, for example, providing access to weapons of mass destruction. Such illicit access then enables the recipient countries to project greater power on the international stage in pursuit of their national interest. Likewise, sanctions violators can

[131] Bratt, interview. Bratt formerly served as Deputy Chief for Export Control and Sanctions at USDOJ's Counterintelligence and Export Control Section as well as Deputy Chief of the National Security Section in the US Attorney's Office for the District of Columbia.

aid host countries in gaining access to otherwise unavailable international financial markets and trade. Therefore, host countries have a strong interest in protecting rather than handing over these defendants.

Even when these offenders leave their safe havens and are apprehended abroad, I learned that their home countries have sought to interfere in the extradition process.[132] As in cybercrime, this interference has sometimes involved launching a competing extradition request. I also heard from law enforcement officials how other times, host countries have placed pressure on the third country to deny extradition.

Nevertheless, we must be aware that prosecutors may have an incentive here to overstate the difficulty of laying hands on these perpetrators in order to justify taking unilateral action. Despite these concerns, host countries' efforts to protect export control and sanctions violators have been independently documented by media reporting in multiple notable prosecutions.

Majid Kakavand was one such defendant who benefited from the interference of his home country: Iran. Between 2006 and 2008, Kakavand and two associates allegedly ran a front company in Malaysia. The company purchased electronic components from the US and Europe, sent them to Malaysia, and then illicitly re-exported them to Iran over 30 times. Two of the ultimate destinations were the Iran Electronic Industry and Iran Communications Industries, both suppliers of the Iranian military. In fact, these companies have been flagged for procuring supplies for Iran's ballistic missile and nuclear programs. These actions violated the US embargo on Iran and its export controls.[133]

In March 2009, Kakavand travelled to Paris on what he intended to be a vacation. However, he was arrested on an US extradition request as soon as he landed. Surprisingly,

---

[132] Bratt.
[133] Albright, Brannan, and Stricker, "Case Study - Middleman Majid Kakavand Arrested for Malaysia-Based Iranian Illicit Procurement Scheme."

the French prosecutor assigned to the case argued against extradition, a view which the French courts ultimately adopted. Digging deeper revealed that Iran had simultaneously offered to free a French citizen who had been jailed in Iran.[134] While France denied that this proposition influenced their decision making, one US official highlighted, "'[Iran] put enormous pressure on the French government, and looming in the background of this is the dangling of a potential prisoner swap.'"[135]

Similar to in cybercrime, China has adopted even more retaliatory means of interfering with extradition requests. In December 2019, Canadian police arrested the Chief Financial Officer of Huawei, Meng Wanzhou. They were acting on US charges that she had "conspired to commit bank fraud by concealing links between Huawei and two shell companies that it used to conduct business in Iran, enabling Huawei to access the dollar-based financial system in violation of US secondary sanctions."[136] China's response was swift. It arrested two Canadian citizens in China on national security charges and sentenced a Canadian convicted of drug trafficking to death. The message to Canada was clear: deny the US extradition request or risk further retaliation against its citizens.[137]

As a result, export control and sanctions cases must find a way to smoke perpetrators out of safety to countries that will reliably assist. I discovered this can oftentimes mean a lure operation. Chief Bratt observed that out of all national security prosecutions, lures are used most frequently in export control and sanctions cases.[138]

For example, in 2007, a prolific Iranian arms acquisitions agent, Amir Hossein Ardebili, was lured to justice. He had made a name for himself by arranging the illicit export of military-use items. These included gyro chip sensors for advanced aircraft and

[134] Erlanger and Audi, "France Won't Extradite Iranian Sought by U.S."
[135] Quoted in Erlanger and Audi.
[136] Keitner, "Trump, Huawei, and the Politics of Extradition: Making Sense of the Meng Case."
[137] Keitner.
[138] Bratt, interview.

missiles, phase shifters for radars in military target acquisition and missile guidance systems, and replacement computers for Iran's F-4 fighter aircraft.[139]

However, Ardebili was based in Iran. There was no chance of an extradition or informal handover. Why would Iran cooperate? This conduct directly benefited them in improving their military capabilities. The lead prosecutor, former Assistant US Attorney (AUSA) David Hall, noted that Ardebili procured these items "directly for the Iran Electronic Institute, the organization that acquired electronic components for the government of Iran."[140] Ardebili was also interested in procuring proliferation equipment for nuclear weapons, clearly within Iran's state objectives at the time. Even if Ardebili was arrested while traveling, Hall was concerned that Iran would seek to interfere in the extradition process.[141]

As a result, law enforcement resorted to a lure to ferret Ardebili out of Iran. Using an existing undercover operation, federal agents negotiated with Ardebili to sell him 1,400 of those phase shifters. The next step was to arrange a face-to-face meeting where they convinced Ardebili that they would deliver the merchandise. Law enforcement settled on the country of Georgia. Little did Ardebili know, Georgia had agreed to extradite him to the US even though there was no extradition treaty. When Ardebili met the undercover operatives there to finalize the deal, local authorities swooped in to arrest him. He was extradited to the US several months later.[142]

Despite these examples, I learned that law enforcement often can catch a break in export control and sanctions cases. They can more reliably wait for perpetrators to travel to friendlier jurisdictions. Chief Bratt explained that the individuals targeted for criminal

---

[139] "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases (January 2009 to the Present: Updated May 13, 2015)."
[140] Hall, *CRACK99: The Takedown of a $100 Million Chinese Software Pirate*, 131.
[141] Hall, *CRACK99: The Takedown of a $100 Million Chinese Software Pirate*.
[142] Hall.

prosecution here are typically procurement agents and businessmen. These defendants frequently travel to inspect merchandise and finalize deals. This international movement provides the perfect opportunity for them to be arrested and rendered from third countries. In fact, there have been multiple successful extraditions of these perpetrators who have travelled to Australia, Singapore, and Malaysia.[143]

Granted, when these individuals are located abroad, a successful extradition is not guaranteed. Chief Bratt explained to me that dual criminality can present a real challenge. The country where the perpetrator is arrested may not have implemented the same export controls or sanctions. Although the item may be recognized as a sensitive commodity, it may not be covered under one of the international export control regimes. So, the arresting country may not view its sale as unlawful.[144] Additionally, US export controls are often based on presidential national emergency powers, which technically only provide temporary authorization. Other countries may not have the same types of laws or may be reluctant to grant extradition based on presidential emergency authorizations.[145]

As an example, Chief Bratt pointed to the prosecution of Ali Asghar Manzarpour. He stood accused of attempting to export a Berkut 360 experimental aircraft to Iran via the UK in violation of the US embargo. He was also alleged to have exported electrical components from the US to Iran via Austria. Based on his emails, law enforcement determined that Manzarpour had travelled to Poland. They tracked him to an internet café in Warsaw and issued a provisional arrest warrant. Polish police apprehended him at the airport, and his extradition was originally approved. However, Manzarpour appealed the

[143] Bratt, interview.
[144] Bratt.
[145] Arnold and Salisbury, "The Long Arm: How U.S. Law Enforcement Expanded Its Extraterritorial Reach to Counter WMD Proliferation Networks," 34.

decision and won. The Polish courts found that his actions did not violate Polish law, and the extradition request failed to meet dual criminality requirements.[146]

These problems of dual criminality have been exacerbated in recent years following the Joint Comprehensive Plan of Action on Iran. Prior to that agreement, most European countries had in place their own sanctions against Iran. This enabled dual criminality to be satisfied if a sanctions violator was arrested in their jurisdiction. Following the deal, many of these sanctions were lifted.[147] AUSA Hall also noted, "A lot of European countries, for example, … in fact, most of them don't have a total embargo on Iran like we do."[148] So, when the US has sought extradition for individuals who violate the US sanctions or embargo, extradition has been denied for a lack of dual criminality.

Nevertheless, these dual criminality concerns can typically still be resolved within the extradition regime. Prosecutors can simply charge additional offenses, such as money laundering and fraud, as part of the indictment. These more basic crimes are then likely to satisfy dual criminality requirements with any country.[149] Based on the rule of specialty, this means that the defendant could only be prosecuted for those common offenses and not the export control or sanctions violations. However, this more limited prosecution still provides a means to bring the individual to justice and hinder the flow of illicit goods.

In many ways, the political challenges to export control and sanctions prosecutions mirror those in cybercrime cases. For both sets of crimes, the most pernicious offenders operate in uncooperative jurisdictions. It's the same countries of China, Iran, and North Korea that provide safe haven to both cybercriminals and export control and sanctions defendants. It's the same countries that act as state sponsors of this illicit conduct. And it's the same countries that seek to interfere in the extradition process when the perpetrators

[146] Bratt, interview.
[147] Bratt.
[148] Hall, interview.
[149] Bratt, interview.

are arrested abroad. In export control and sanctions cases, a principal solution has been a sustained effort to lure these individuals to the US or countries that will reliably render them. This suggests that a similar outcome will be necessary for cybercrime.

Despite these shared challenges, cybercrime is different from export control cases on certain key dimensions. In fact, these differences create an even greater need for unilateral action in cybercrime. Primarily, as we learned in Chapter 4, cybercrime is inherently a law enforcement, not foreign policy, matter. These offenses are usually inflicting serious and continuing economic harm on the victims. Thus, there is a pressing need to arrest and neutralize the threat actor in order to stem the financial losses.

This contrasts with export control and sanctions cases where there are no tangible victims suffering ongoing harms. The central goal of the prosecution is to achieve a foreign policy objective, such as depriving a rival state or terrorist group of sensitive technology. While these are important considerations, other tools can be brought to bear on the problem with more immediate effect, such as intercepting shipments. Indeed, a criminal prosecution may have little impact since the recipient country or group may simply turn to another procurement agent. Even if there are many cybercriminals launching attacks, the prosecution of just one offender can still stop his victims' bleeding.

Additionally, there is no significant attribution challenge in export control and sanctions cases. These perpetrators are businessmen brokering international transactions, which leaves a trail of evidence leading to their true identity. They are frequently interacting and meeting with prospective sellers of the sensitive commodities. This need for communication not only offers evidence of the criminal conduct but also introduces the possibility of flipping co-conspirators into cooperating witnesses. Conversely, in cybercrime, law enforcement struggle to prove who committed the offenses. After all, cybercriminals frequently operate using only nicknames. Even if the attack can be traced

to a specific computer, it remains difficult to prove who was using the device. So, law enforcement has a further reason to lure cybercriminals: to establish their identity.

Moreover, in export control and sanctions cases, law enforcement can typically wait for defendants to travel on their own volition. However, there is no business reason for cybercriminals to travel. They can execute their conspiracies entirely from the comfort of their home countries. Hence, law enforcement must smoke them out of hiding.

Indeed, the lack of a business need for face-to-face interaction may make a lure operation more difficult in cybercrime. Perpetrators may be wary of meeting in person. Nevertheless, law enforcement can simply change the angle of the lure. They can play off the vanity or ego of cybercriminals by offering fake jobs like in the Ivanov and Gorshkov case, inviting them to conferences, or even enticing them with sex as seen in the Dolan and Butu case. One prosecutor remarked to me that the skills to commit cybercrime are quite marketable for legitimate employment, so job offers are believable.[150] As the case studies recounted in Chapter 4 clearly demonstrate, cybercriminals can be incentivized to travel with the proper inducements.

Cybercriminals may also be more prone to falling for ruses than export control or sanctions defendants. They can be overconfident in their ability to conceal their identity. The anonymity of the internet, combined with their own hubris, can create a false sense of security. This means that they may underestimate the risks of agreeing to travel when presented with the right enticements.[151] The anonymity of the internet can further facilitate lures since cybercriminals are accustomed to dealing with individuals whom they have never met yet still developing trust. This provides an avenue to introduce an undercover investigator and carry out a lure operation.

[150] Prosecutor 9, interview.
[151] Prosecutor 9.

In export control and sanctions cases, it is significantly more difficult for law enforcement to gain access to the perpetrator and develop trust. As in the Ardebili case, they may need a cooperator to facilitate an introduction and vouch for them, which can be challenging to attain. Comparing his experiences luring both a cybercriminal (Li) and export control violator (Ardebili), AUSA Hall reflected that the cyber aspect of the Li case "made it a little easier in the sense that there's an obvious point of entry. Whereas [in the Ardebili case] actually making initial contact with him was difficult."[152]

5.5 Concluding Remarks

This chapter has examined the experiences of securing custody over perpetrators located abroad for four key areas of transnational criminality. My interviews with law enforcement officials suggest that unilateralism is the exception rather than the norm for each of these other transnational crimes. They predominantly proceed through cooperation with the host country or waiting for the defendant to travel. This means that they each face a lesser need for unilateral alternatives to extradition compared to cybercrime. However, their successes are not likely to be witnessed in cybercrime prosecutions any time soon.

Terrorism was originally handled as a military matter, allowing these cases to proceed through extrajudicial mechanisms. As the emphasis shifted to criminal prosecutions in the mid-2000s, the US maintained a preference for foreign countries to prosecute. These individuals could pose a public safety risk if incarcerated in US prisons. The cases that have been prosecuted in US have typically relied on quasi-extraditions or extraditions since host countries share an interest in holding these offenders accountable. Additionally, terrorism has been near universally condemned, facilitating cooperation.

Yet, in cybercrime, the benefits to host countries and lack of consensus mean that host countries do not have the same interest in cooperation. They rather shield or coopt the

[152] Hall, interview.

perpetrators. The military route is also off the table since cybercriminals reside in governed spaces, the perpetrators are not enemy combatants, and the law of armed conflict does not apply. Hence, cybercriminals cannot be snatched off the street or neutralized using a drone strike without risking retaliation and likely breaching international law.

Drug trafficking cases once relied on unilateral captures to bring perpetrators to justice. At the time, host countries were legally prohibited from extraditing and did not have adequate institutions to domestically prosecute. But this all changed as legal reforms were inaugurated in the most prolific host countries and the US pumped in foreign aid on the condition that host countries hand over drug traffickers. Now, these cases rely on cooperation from host countries or waiting for traffickers to travel to friendly jurisdictions.

Unfortunately, such a transformation will not likely be possible in cybercrime. The challenges to cooperation are political, not legal, so they cannot be resolved through legal reform. Cybercriminals also do not target their fellow countrymen, which mitigates host countries' interests to cooperate. And foreign aid is not politically feasible given the strained relationships with the most prolific host countries. Furthermore, cybercriminals do not travel on their own, precluding a wait and see approach.

Turning to fraud and foreign corruption, these prosecutions have not needed to depend on unilateral alternatives. The defendants are international businessmen who do not wish to have international arrest warrants or Red Notices hanging over their heads. So, many waive extradition. They can also be arrested when travelling. Even if they never leave their country of residence, host countries have reliably extradited the perpetrators.

This experience is not likely to be replicated in cybercrime since the perpetrators have no business reason to travel. They are also oftentimes incentivized to challenge rather than assent to extradition since they can easily claim "some other dude did it" and may fear a potential lengthy prison sentence. Furthermore, cybercrime cases prioritize

prosecuting individuals rather than corporations, which makes securing custody a more pressing concern than in fraud or corruption cases.

Export control and sanctions cases face similar political challenges to cybercrime. The perpetrators tend to reside in safe haven countries that have every incentive to protect them. This even results in host countries interfering in the extradition process when offenders are arrested in third countries. Thus, law enforcement must at times apply lure operations to entice defendants to the US or territories from where they can be successfully rendered.

Given the shared political obstacles, the experience of export control and sanctions prosecutions suggest that cybercrime will also face a sustained need for unilateral alternatives. In fact, there are certain key differences that suggest the need will be even higher in cybercrime. Cybercrime is predominantly a law enforcement, not foreign policy, matter with tangible victims. Therefore, the priority is on arresting the defendant to stem the ongoing financial losses. Plus, cybercriminals can easily hide behind the anonymity of the internet, which may require a lure operation to establish their identity. And, unlike export control and sanctions violators, cybercriminals do not travel as part of the conspiracy, so they must be smoked out of hiding.

These predictions for the future of cybercrime raise important legal and policy questions. How can we ensure that unilateralism does not run amok? Under what conditions may the use of such tools be prudent? These questions will be explored next.

6. OUTLINING AN INTERNATIONAL FRAMEWORK FOR THE USE OF UNILATERAL LURE OPERATIONS IN CYBERCRIME PROSECUTIONS

Hostis humanis generis, the enemy of all mankind. For a span of centuries and in nearly all corners of the globe, piracy plagued the high seas. Ships carrying precious cargo sailed under the omnipresent threat of attack by armed marauders. Sailors risked life and limb as countless were killed or taken hostage by sea raiders. Freedom of movement and international trade were endangered by this criminal industry.

The menace of international piracy was particularly insidious due to the pervasive level of state sponsorship. Pirates must land somewhere; they cannot spend eternity lurking the seas. However, victim countries could not turn to pirates' home countries for assistance. Certain host countries directly benefited from this sea raiding and thus provided their support.

In the Mediterranean, the Barbary Coast of Africa was a hotbed for marauding between the 16th and 18th centuries. These corsairs operated with such a level of support from their home countries that European countries often struggled to identify whether they were pirates or belligerent warships.[1] The sovereign Barbary states, in turn, enjoyed the protection of the Ottoman Empire, which enabled piracy to flourish during this period.[2]

Around the globe in South East Asia during the heyday of piracy from 1750 to 1860, "maritime marauding was one of the key strategies used by political leaders to expand their prestige, wealth, and power."[3] Local rulers commonly provided pirates with weapons and opium. In exchange, they expected a portion of the plunder and bounty.[4]

---

[1] Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*, 110.
[2] Horsley, "State-Sponsored Ransomware Through the Lens of Maritime Piracy," 674.
[3] Antony, "Turbulent Waters: Sea Raiding in Early Modern South East Asia," 32.
[4] Antony, 34–35.

Within the region, Borneo was one of the most pernicious sources of piracy. When the sultan of Brunei attempted to collaborate with the British on combatting this scourge, his opponents threw him out of office and "replaced him with a 'puppet of the pirates.'"[5] Piracy became so intertwined with state objectives in the region that during an 1838 trial of Iranun pirates, the perpetrators "'appear[ed] to consider themselves, in fact, as having been engaged in the lawful discharge of their duties as subjects of his highness of Soloo.'"[6]

Additionally, certain host countries disagreed with European notions on the morality of piracy. Instead of a criminal enterprise, they often viewed it as a "respectable profession."[7] In fact, Sultan Husain of Singapore once declared that the activities deemed piracy by European countries "'brings no disgrace' to Malay rulers."[8] As a result, they did not share Europe's political interest in addressing this conduct.

This narrative only scratches the surface of the blended threat of piracy and challenges of bringing these perpetrators to justice. European countries simultaneously sponsored their own acts of piracy. They attempted to legitimize and legalize this conduct under the guise of issuing charters to so-called privateers, like Queen Elizabeth I to Sir Francis Drake. However, their conduct was substantively no different.

Since victim countries could not turn to pirates' home countries for assistance, unilateralism became the norm. Victim countries launched missions to destroy pirates' forts, ships, and bases and even summarily execute the perpetrators. In one naval operation in Brunei, "more than eight hundred pirates were killed or drowned. This expedition

[5] Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*, 114.
[6] Benton and Ford, *Rage for Order: The British Empire and the Origins of International Law, 1800-1850*, 136.
[7] Antony, "Turbulent Waters: Sea Raiding in Early Modern South East Asia," 25.
[8] Antony, 25.

effectively put an end to Borneo piracy."[9] Elsewhere in South East Asia, "subdued pirate communities were forcefully resettled in new areas away from their original power bases."[10]

Ironically, an empire that burst onto the world stage through piracy against Spain, the British Empire, led the charge. During the 19th century period of *Pax Britannica*, "Britain's maritime forces, including armed merchantmen, East India Company warships, and sloops, schooners, and other light craft, attempted to sweep clean the seas of these corsairs … The British put the pirates out of work; they created unemployment, as it were."[11] By 1860, unilateralism proved so effective that piracy remained suppressed in the region for a century.[12] Yet, in many ways, these efforts can be viewed as unilateralism run amok. The sovereignty of host countries was frequently breached, and pirates faced summary "justice" without any semblance of due process under the law.

Cybercrime can, in many respects, be considered modern-day piracy. Both offenses are truly global in scope. The high seas and World Wide Web are a largely analogous international commons over which no country can assert effective control. Accordingly, both offenses require a coordinated global response to bring perpetrators to justice.

However, victim and host countries oftentimes have divergent interests. Instead of supporting pirate attacks against ships for booty, certain host countries now enable and sponsor cyberattacks against foreign citizens and businesses. Instead of questioning the morality of marauding, other host countries now question the wrongfulness of cybercrimes. Instead of pirates hiding behind "the elusiveness and anonymity of a ship in

[9] Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*, 114.
[10] Antony, "Turbulent Waters: Sea Raiding in Early Modern South East Asia," 36.
[11] Gough, *Pax Britannica: Ruling the Waves and Keeping the Peace before Armageddon*, 200.
[12] Antony, "Turbulent Waters: Sea Raiding in Early Modern South East Asia," 36.

the expanse of the ocean," cybercriminals now hide behind the anonymity and expanse of the internet.[13]

Although cybercrime has not posed the same threat to human life as piracy, its non-violent nature can present its own complications. Certain host countries do not consider these offenses important enough and lack the political will to assist. The stakes seem lower, so host countries can take a stand and deny extradition for domestic political gain.

In Chapters 4 and 5, I presented arguments that these challenges create a heightened need for unilateral approaches in cybercrime as compared to other transnational crimes. Furthermore, cybercrime is not likely to evolve toward cooperation in the same manner as other transnational crimes. If unilateralism is indeed here to stay, what is to prevent it from running amok as in the early years of piracy enforcement?

Without countries exercising self-restraint and responsible behavior, such efforts may unduly violate the sovereignty of host countries, infringe upon the human rights and due process of the accused, and undermine respect for international law and cooperation. At the same time, these concerns must be balanced against the need to end ongoing cybercriminal conduct, defend the interests of victims, and deter future attacks. This suggests that there are limited circumstances where unilateralism may be advisable.

The goal of this chapter is to outline baseline standards for when unilateralism, in the form of lure operations, may be prudent in cybercrime cases. While this framework is informed by international law, it does not seek to settle longstanding debates in international law on unilateralism. Rather, it serves as a pragmatic public policy guide for pursuing countries to consider when their lures are likely to provoke criticism from human rights and/or international law advocates. These standards also do not limit or prohibit action that may otherwise be consistent with international law. Thus, if countries choose to

[13] Anderson, "Piracy and World History," 178.

depart from the framework, their actions are not necessarily impermissible or unlawful. The use of the lure simply entails a greater risk of backlash from elements of the international legal and political community.

While this study has focused on the United States, it is not the only country with equities in the arrest and prosecution of international cybercriminals. Third countries may also have an interest in the outcome. They may benefit from the spillover effects of lure operations. Cybercriminals often target entities in multiple countries, so a lure can immediately end cyberattacks against victims in those third countries. After completing their sentence, these cybercriminals can likewise be extradited to other victim countries.

The use of lure operations is not reserved to the US either. Indeed, through my interviews with law enforcement officials from other countries, I learned that Belgium, Germany, and Israel have all previously utilized lures.[14] In fact, at least Israel has done so in a cyber-related case. Amos Silver, a dual citizen of Israel and the US, was accused of running Telegrass. This cannabis trading marketplace served hundreds of thousands of Israelis through the encrypted messaging app, Telegram.[15] But, Silver was living in Miami. Extradition attempts with the US had failed, so he was beyond the reach of Israeli law enforcement.[16] Or, so he thought. Israeli law enforcement launched a lure operation to arrest him. An undercover agent pretended to be a fan and invited Silver to a wedding in Kiev, even purchasing his airfare. Instead of enjoying the festivities, Silver was arrested soon after he arrived and extradited to Israel.[17]

Therefore, my framework is not drafted from a US perspective or intended to solely apply to the US. Rather, it is written from a neutral position. It aims to offer

[14] Kerkhofs, interview; German Prosecutor, interview; Israeli Law Enforcement Official, interview.
[15] Genesove, "The Highs and Lows of Amos Silver, Telegrass Cannabis Kingpin Nabbed in Ukraine."
[16] Israeli Law Enforcement Official, interview.
[17] Genesove, "The Highs and Lows of Amos Silver, Telegrass Cannabis Kingpin Nabbed in Ukraine."

recommendations on the use of lure operations to any government, particularly since other countries like Belgium, Germany, and Israel already deploy such unilateral alternatives.

I begin by examining the conditions that the US follows in deploying lures to determine if any lessons can be learned. Following the infamous Alvárez-Machaín case discussed in Chapter 5, I learned that the US has implemented a centralized approval process for unilateral alternatives, including lures. Martha Stansell-Gamm, who was Chief of the US Department of Justice's (USDOJ) Computer Crime and Intellectual Property Section (CCIPS) from 1999 to 2007, explained to me that lures were rare and to be used only when "there was no other realistic possibility that any country would impose criminal sanctions and even then, there were important legal and political factors to weigh."[18]

For example, lures are only employed for a "continuing and ongoing threat" that risks causing significant damage.[19] Furthermore, lures must not entrap or coerce the defendant, who is then guaranteed a US criminal trial with all its procedural protections. Nevertheless, I discovered that USDOJ previously interpreted the definition of a lure so narrowly as to create a major loophole from the approval process. While this has now been rectified, other countries should not adopt the same loophole in their review of lures.

I then assess existing justifications in the international law literature related to the use of unilateral alternatives to combat other crimes since such arguments have not yet been advanced for cybercrime. I first find that the International Criminal Tribunal for the former Yugoslavia (ICTY) has provided law enforcement with broad powers to bring war criminals to justice. This court has ruled that lures do not violate the sovereignty of host countries nor the rights of the accused since his travel is voluntary. Even in cases where

[18] Stansell-Gamm, interview.
[19] McCord, interview, August 14, 2019.

the defendant is abducted rather than extradited, the ICTY has ruled the trial may proceed so long as the capture does not involve egregious abuses, such as torture.

Nevertheless, war crimes are not the same as cybercrimes. There is a marked difference in the severity and level of condemnation of these offenses. Plus, the ICTY is distinct from a national court. It was constituted by the United Nations Security Council. So, a unilateral alternative to enforce its arrest warrant may entail less of an infringement on the host country's sovereignty than if such an action were taken by a pursuing country.[20] While precedents from war crimes prosecutions may help establish minimum standards for lure operations in cybercrime, the differences between these offenses suggest that further restrictions may be wise.

As a result, I then look to a crime that is not yet considered a universal offense and that is prosecuted by national courts rather than international tribunals: terrorism. International legal scholars have advanced a number of arguments supporting the legality of unilateral alternatives here based on theories of self-defense, necessity, due diligence, and efficient breach. These justifications collectively suggest that unilateralism should only be applied when it is necessary as a last resort, there is an imminent and significant threat, the unilateral response is proportionate, and the host country is complicit.

It's important to note that unlike most cybercrimes, terrorism is a violent offense that poses a direct threat to human life. This suggests that there should be an even higher threshold for unilateralism in cybercrime. Indeed, certain interpretations of the self-defense doctrine would not apply to cybercrime. Yet, these legal justifications in terrorism have been advanced for capture operations, which entail a much greater intrusion on the sovereignty of the host country and human rights of the accused. This suggests a lure

[20] Sridhar, "The International Criminal Tribunal for the Former Yugoslavia's Response to the Problem of Transnational Abduction," 355.

would require a lower threshold, which mitigates against cybercrime's nonviolent nature and supports applying similar standards from terrorism cases. However, the final requirement of complicity should be relaxed for cybercrime due to the attribution challenge, which is less of a complication in terrorism cases. Relinquishing lure operations as a tool to help establish the perpetrator's identity would allow devastating cybercrimes to continue unpunished.

Finally, I examine an area of transnational criminality that does not necessarily entail violence: drug trafficking. The existing scholarship in this area espouses a similar logic to the defenses of unilateralism in terrorism. When host countries fail to combat this threat or actively partake, victim countries can engage in self-help through unilateralism. There simply must be no other remedy, and the unilateral response must be proportionate to the threat. The literature has also highlighted that unilateralism is more justified for drug trafficking since the crimes are for the private benefit of the perpetrators. This raises questions for cybercrime, particularly given the role of state sponsorship.

Applying these lessons from the US example and international law, I propose the following framework as to when the use of unilateral lure operations may be advisable in cybercrime cases.

First, there is no viable and less intrusive alternative to secure custody.[21] The perpetrator's identity may not be known. Or, he may reside in a safe haven country and not reliably travel to more cooperative jurisdictions. This means that the lure would indeed be necessary as a last resort.

Second, the cybercriminal poses a significant and imminent threat. Otherwise, the lure would risk causing international strife over a minor incident and would not be a

[21] For example, a capture operation may be another viable alternative, but it would be more intrusive and present a greater breach of international law. Therefore, the presence of this option does not preclude a lure operation.

proportionate response. Additionally, if the harm is not imminent, the pursuing country has greater flexibility to wait, for example, for the defendant to travel, to develop stronger evidence, or for the host country to change its political stance in favor of cooperation.

Third, the conduct is suspected to be for the private gain of the perpetrators. In cybercrime, this may manifest as economic profit, personal learning, or personal entertainment. This indicates that lure operations would not be advisable for conduct that is motivated by a political objective, such as political speech online. Ordinarily, extradition would be prohibited for such conduct. Therefore, allowing a lure would risk circumventing one of the defendant's key due process protections. It's important to note that even if wily cybercriminals attempt to commit politically motivated cybercrimes as cover, a lure would still be permitted to prosecute any conduct for their private gain.

This condition also indicates that it would not be prudent to deploy a lure against a state official for acts performed in an official capacity. Under customary international law, state officials typically enjoy functional immunity (*ratione materiae*) from criminal prosecution by foreign courts for any act performed in the exercise of state authority. US officials have asserted that such immunity does not apply when the crime takes place on US territory. Yet, this issue is not settled under international law. So, deploying lures here risks undermining international stability and setting a dangerous precedent that would allow countries to prosecute any cyber intrusions in their territory, even those for traditional espionage purposes.

Fourth, the lure does not engage in entrapment or coercion. This means that law enforcement can provide an opportunity for the suspect to commit cybercrimes or grow an ongoing conspiracy. However, they cannot unduly urge, harass, or strongarm him to break the law. Nor can they threaten he or his loved ones to compel him to travel. These

restrictions will ensure that the defendant's travel is truly voluntary, in line with the international court precedent.

Fifth, the lured perpetrator is guaranteed a fair trial upon arrest, which includes access to consular assistance.

This chapter proceeds as follows. Section 6.1 explores the safeguards that the US has applied for lure operations to determine whether any lessons can be learned. Sections 6.2, 6.3, and 6.4 surveys the legal justifications that have been advanced for unilateralism in war crimes, terrorism, and drug trafficking prosecutions to examine their applicability to cybercrime. Section 6.5 outlines the international framework that I propose for the use of unilateral lure operations in cybercrime cases.

6.1 Lessons from the US Example: What Safeguards Exist?

In this section, I describe the checks that the US has implemented on the use of unilateral lure operations as well as the shortcomings that must not be repeated. Since the Álvarez-Machaín case, prosecutors reported that the US has implemented a "pretty selective and burdensome" approval process for unilateral alternatives, including lures.[22] They repeatedly emphasized that there are not just individual agents and prosecutors running around and executing lures.[23] There is a "system in place for quality control."[24] This approval process could inform the development of an international framework as to when the use of lures may be prudent. Nevertheless, are the US review protocols truly that rigorous and protective of defendants' rights?

According to the Justice Manual, any prosecutor who wishes to employ a lure must submit a formal memo to USDOJ's Office of International Affairs (OIA). If OIA approves the memo, it is passed on to the Deputy Assistant Attorney General for International

[22] Prosecutor 18, interview.
[23] Prosecutor 18; Prosecutor 45, interview; Prosecutor 32, interview.
[24] Prosecutor 18, interview.

Affairs for final sign-off.[25] Throughout this process, the prosecutors and OIA will confer with the Department of State and the US Ambassador in the host country to mitigate any diplomatic blowback. If the perpetrator is lured to a third country, that country will also be notified and consulted. However, just because a procedure is codified in a manual does not mean it is followed in practice. So, I questioned prosecutors as to whether any approvals are necessary for a lure operation. While many could not recall all the details of the process, they consistently referred to consulting with OIA. Prosecutors would then rely on the guidance of OIA on the necessary steps, such as the lure memo and internal reviews.

Overall, interviewees shared with me that the review process is guided by an interest in maintaining due process and ethical standards. One prosecutor explained to me:

> [When] we're using trickery to effectuate an arrest, there's always a concern about a sense of fair play in whether or not we're acting appropriately. So, we always want what we're doing [to be] something that we would feel comfortable from an ethical perspective and also from a political perspective. So, we have to be extremely careful … we're always trying to be fair and make sure people are entitled to whatever due process they're entitled to in the relevant country.[26]

There is a risk here that prosecutors may overstate their concern for defendants' rights to escape any negative perceptions. Nevertheless, adhering to ethical standards would also be within their self-interest. If an egregious violation were to occur, there is a risk it could come out at trial and jeopardize the chances of conviction. And it could lead to significant adverse media attention, which could jeopardize USDOJ's reputation and critical relationships with foreign law enforcement partners. This precise scenario occurred in terrorism cases over the use of Guantanamo Bay.

Even if prosecutors genuinely strive to maintain "a sense of fair play," we must still interrogate how specifically the review process accomplishes that goal. I learned that OIA scrutinizes the content of the lure so that it does not border on entrapment.

---

[25] "9-15.000 - International Extradition and Related Matters."
[26] Prosecutor 57, interview.

Entrapment occurs when law enforcement induces an individual to commit a crime through threats, harassment, or trickery. This is distinct from merely providing a defendant with the opportunity to commit a crime or further his conspiracy in line with his existing intent. In other words, the government's actions cannot be the primary impetus for the criminal conduct by unduly urging or harassing the individual to violate the law. This distinction has traditionally been based on the premise that innocent individuals would reject an opportunity to break the law but may not reasonably be able to resist coercion.

Generally, this is not a concern for lure operations since the defendant has already committed his crimes, and sufficient grounds for arrest already exist.[27] Prosecutors are not charging the accused based on his actions in response to the lure. Rather, the lure is simply about getting him to leave his safe haven.

But what about those lure operations, such as in the CRACK99 case from Chapter 4, that involve ongoing undercover investigations with law enforcement posing as co-conspirators? Cases like that may blur the line and risk entrapping the defendant. However, prosecutors shared with me that they will "construct the lures pretty carefully so it doesn't appear that you're actually inducing them to commit a crime in that jurisdiction."[28] This observation is supported by the CRACK99 case. The defendant, Xiang Li, had independently committed cybercrimes far before the undercover investigation, creating probable cause for arrest and precluding any entrapment concerns.

Law enforcement officials also explained to me that OIA ensures that the lure is not coercive. This concern is distinct from entrapment, which is about forcing or inducing the accused *to commit a crime*. A coercive lure is about forcing the defendant, who may have already committed a crime, *to travel outside his home country*. This means, for

[27] Prosecutor 18, interview.
[28] Prosecutor 17, interview.

example, that law enforcement cannot threaten the defendant or his loved ones if he refuses to travel. Dave Denton, the then Deputy Assistant Director for the Cyber Division of US Homeland Security Investigations, elaborated that lures also cannot limit the defendant's options or offer an enticement that would be too good to pass up.[29]

But, could law enforcement officials have shared this criterion with me merely to make the US use of lure operations appear ethical? I found that it is indeed applied in practice. In the Dolan and Butu case, federal agents devised a plan to lure one of the other co-conspirators, Adrian-Tiberiu Oprea. Oprea knew that Dolan had travelled to the US. So, after arresting Dolan, agents came up with the idea to pretend to be him, contact Oprea, claim that Dolan was in an accident, and ask Oprea to visit him in the US. However, this plan was quickly rejected.[30] The lure would have been unduly coercive by creating the appearance that a close friend was in jeopardy.

Equally important, I learned that the approval process ensures that lures are only used as a last resort. One prosecutor explained to me, "A lure is not our first action. In fact, part of the authorization process is that you've eliminated the other options … That's not to say agents won't come up with a lure as the first option they want … [But] we have to say no, there are options that we have to pursue before we consider it."[31] Extradition must not be possible. The host country must not be expected to cooperate informally or prosecute domestically. And the defendant must not be expected to travel on his own volition. Twenty-one of the prosecutors and federal agents I interviewed agreed with these observations. This was further supported by the case studies. In none of the lure operations I reviewed was there another viable way to secure custody.

[29] Denton, interview.
[30] Federal Agent 11, interview, August 22, 2019.
[31] Prosecutor 29, interview, August 13, 2019.

Moreover, lures must only be used for significant cases. Former cybercrime prosecutor and diplomat Chris Painter elaborated that it must be a "big case with lots of damage, lots of dollar loss, lots of victims."[32] Twenty-three other prosecutors agreed with this assessment. The significance of the case is likewise judged in terms of whether the cybercriminal poses a continuing threat.[33] As one prosecutor observed, "one and done is not going to cut it for a lure."[34] For example, in the Dolan and Butu case, a federal agent recollected, "I could see every hack that they were trying to do, and I would call every day dozens of businesses and let them know that they've been compromised. In about four months, they got into over 800 victim merchants."[35] The significance of the case can also be determined based on whether the cybercriminal is a repeat offender.[36]

Even with this review process, there are legitimate concerns that the US may use lures to advance geopolitical or national security objectives. This is particularly pertinent for cases involving state sponsorship. However, as we learned, the US has focused on only prosecuting cyber conduct "that's straight up criminal" regardless of "whose badge or uniform [the defendant is] wearing."[37] Assistant Attorney General for USDOJ's National Security Division John Demers explained, "We understand that nations have engaged in political, military espionage for thousands of years, and if you look at our charges, you'll see that we have not charged that kind of activity even though we're quite aware of it and we try to combat it in other ways."[38] While prosecutors may have an incentive to hide any political usage of lure operations, the empirical record supports these observations. A

[32] Painter, interview.
[33] Prosecutor 10, interview.
[34] Prosecutor 29, interview, August 13, 2019.
[35] Federal Agent 11, interview, August 22, 2019.
[36] Prosecutor 17, interview; Prosecutor 2, interview; Prosecutor 23, interview.
[37] Prosecutor 28, interview, August 9, 2019.
[38] Carlin, "Cyber Space with John Carlin (Ft. John Demers)."

review of all known cybercrime prosecutions involving lure operations confirmed that this tool has only been used against private individuals in cases of purely criminal conduct.

The defendant's rights are further preserved since he is entitled to all the protections of a US criminal trial. He has the right to remain silent, have legal counsel, and have his case decided by a jury of twelve citizens. He can also review any potentially exculpatory evidence and mount a rigorous defense. As one prosecutor relayed to me, "we believe in our own system, and it's a rigorous one with a lot of rights and freedoms … When they come to the US, they get the benefit of all of our protections."[39]

Despite these safeguards, the US example raises one area of concern. According to the USDOJ Justice Manual, a lure operation is defined as "using a subterfuge to entice a criminal defendant to leave a foreign country so that he or she can be arrested in the United States, in international waters or airspace, or in a third country for subsequent extradition, expulsion, or deportation to the United States."[40] In the past, USDOJ narrowly interpreted this definition to exclude cases where the defendant suggested or selected the travel destination. Those cases were then not subject to the review process, even if the defendant would not have travelled but for the undercover operation.[41]

For example, in one case, the defendant suggested the location. As one prosecutor recalled, "once he suggested going there and made it clear that he was interested in going there on a vacation and we could meet there, it wasn't a lure anymore as far as the Department [of Justice] was concerned, which dramatically reduced the red tape."[42] This red tape was waived even though the defendant was enticed to leave his home country via a subterfuge, irrespective of who selected the destination.

---

[39] Prosecutor 23, interview.
[40] "9-15.000 - International Extradition and Related Matters."
[41] Prosecutor 29, interview, March 19, 2021; Hall, *CRACK99: The Takedown of a $100 Million Chinese Software Pirate*, 200.
[42] Prosecutor 38, interview.

In another case, one prosecutor detailed that the cybercriminal "had a choice as to whether he would [go to] Europe or the United States. And he told the agent, 'I've never been to the US, so I'll come to the United States.' So that was not a lure. It was his decision to do that and leave where he was and come."[43] Although the accused would not have travelled to the US but for the ruse, no lure memo or OIA approval was necessary.

Since these cases, USDOJ changed its position such that any ruse to entice the defendant to travel is considered a lure, even if he suggests or selects the location.[44] Looking forward, it is important to ensure that this loophole does not reemerge. Otherwise, law enforcement officials could skirt the norms of responsible behavior and conduct lure operations that run afoul of legal and ethical standards.

6.2 War Crimes: Minimum Standards for Unilateral Alternatives

Although the US has adopted these restrictions on the use of lure operations, what does the international law literature have to say as to when unilateralism may be justified to bring international and transnational criminals to justice? One area to first explore is war crimes where there have been several cases involving unilateral alternatives. This has generated precedents from the ICTY. In one case, the court ruled that a lure did not violate the sovereignty of the host country or human rights of the accused. Even a capture operation would not provide grounds for setting aside the court's jurisdiction over the accused as long as it did not entail inhumane treatment. However, cybercrime is neither a universally condemned offense nor prosecuted by an international tribunal like the ICTY with powers from the UN Security Council. This suggests that the lessons from these war crimes cases can only help establish minimum standards. Greater safeguards and restrictions will likely be necessary for the use of unilateralism in cybercrime.

[43] Prosecutor 29, interview, August 13, 2019.
[44] Prosecutor 29, interview, March 19, 2021; Prosecutor 53, interview.

Given the heinous nature of war crimes, certain international law scholars have called for solutions akin to unilateral alternatives to extradition. Even though international tribunals exist to adjudicate these violations, they often face the same difficulty as victim countries of cybercrime. The host countries simply refuse to hand over the perpetrators.[45] As a result, in the 1990s and early 2000s, "many of the most notorious indictees of the Yugoslavia Tribunal remain[ed] at large."[46]

To address this worrying trend, one solution proposed in the legal literature was to establish an international bounty system to arrest indicted perpetrators. This would operate like a unilateral capture operation except that it would be carried out by private actors on behalf of the international tribunals. Kovac stipulates that it should only be applied when the host country refuses to extradite or prosecute the accused. Plus, the defendant should not be apprehended in an unduly harsh or abusive manner. The bounty also should not be set until there has been a proper indictment, which provides a measure of due process.[47]

Likewise, Professor Scharf asserts that abductions or lures of war criminals could be justified based on the right of countries under the UN Charter to enter another's territory in self-defense. This would only apply in instances where the war criminal poses a continuing threat and the host country is providing protection or safe haven. He explains that "to the extent indicted war criminals located in the [Federal Republic of Yugoslavia] or Croatia constitute a threat to the NATO or United Nations troops stationed in the territory of the former Yugoslavia, this would provide justification for abducting or luring such individuals for purposes of arrest."[48]

---

[45] Kovac, "Apprehension of War Crimes Indictees: Should the United Nations' Courts Outsource Private Actors to Catch Them," 620.
[46] Kovac, 650.
[47] Kovac, 652.
[48] Scharf, "Case Analysis: The Prosecutor v. Slavko Dokmanovic: Irregular Rendition and the ICTY," 377.

However, when the issue of abductions and lures has been posed to the ICTY, it has adopted a far more permissive standard toward such operations. In 1991, Slavko Dokmanović participated in the largest massacre in the war in Croatia. 261 individuals were forcibly removed from a hospital in Vukovar, Croatia and executed. But, Dokmanović had moved to the Federal Republic of Yugoslavia (FRY), a territory that repeatedly would not carry out arrest warrants for indicted war criminals. Thus, the Office of the ICTY Prosecutor set up a sting operation. One of their investigators convinced Dokmanović that he had organized a meeting for Dokmanović and the Transitional Administrator for Eastern Slavonia. Dokmanović had been forced to abandon property in Eastern Slavonia, which is a region of Croatia, and thought he would be compensated at the meeting. But, to his surprise, once he arrived, he was promptly arrested.[49]

At trial, Dokmanović challenged the circumstances of his arrest as stemming from a lure operation. However, the court ruled that the "'luring' is consistent with the principles of international law and the sovereignty of the FRY."[50] Specifically, the lure did not violate his human rights since Dokmanović was not deprived of his liberty until the moment he was lawfully arrested in Eastern Slavonia. Deprivation of liberty requires that the defendant be in a situation where he knows he is no longer free to leave. This does not apply to a lure operation since the defendant can choose to cancel his travel plans at any time. It only applies once the handcuffs have been placed. Plus, the lure did not violate the sovereignty of the host country (the FRY) since the arrest was carried out in Eastern Slavonia, which is in Croatian territory.[51]

[49] Scharf, 369–70.
[50] Decision on the Motion for Release by the Accused Slavko Dokmanović, *Mrksić et al.* (IT-95-13a-PT), Appeals Chamber, 22 October 1997 [57].
[51] McDermott, "Seeking a Stay of Proceedings for Irregular Apprehension before International Courts," 152, 156.

The ICTY faced a similar question in the case against Dragan Nikolic, its first indictee. Nikolic was charged with war crimes, crimes against humanity, and breaches of the Geneva Convention. He had been the commander of a camp in Bosnia and Herzegovina through which as many as 800 Muslim civilians are estimated to have passed. He was "accused, among other charges, of killing 8 detainees, of torturing 10 others, of causing great suffering or serious injuries to 3 others, and of the deportation, confinement and persecution of more than 500 civilians."[52] In 2000, Nikolic was kidnapped in the FRY by unknown people, transported over the border into Bosnia and Herzegovina, and delivered to NATO forces.

His attempts to challenge the circumstances of his arrest met a similar fate as Dokmanović. The Trial Chamber concluded that it would only stay the proceedings if "an accused is very seriously mistreated, maybe even subjected to inhuman, cruel or degrading treatment, or torture, before being handed over to the Tribunal."[53] This reasoning was upheld by the Appeals Chamber. Combined, the rulings in the Dokmanović and Nikolic cases suggest that only a low threshold should be applied to bar unilateral alternatives. As long as they avoid egregious abuses, the trial may proceed. This is particularly true for lures, which the ICTY deemed less invasive.

Nevertheless, there are critical distinctions between the crimes these men were accused of and cybercrime. Primarily, the Appeals Chamber in Nikolic noted that genocide, crimes against humanity, and war crimes are "universally recognised and condemned as such."[54] Consequently, "the damage caused to international justice by not apprehending fugitives accused of serious violations of international humanitarian law is

[52] "First Witnesses to Give Evidence in Open Court in the Nikolic Case."
[53] Decision on Defence Motion Challenging the Exercise of Jurisdiction by the Tribunal, *Nikolic* (IT-94-PT), Trial Chamber, 9 October 2002 [114].
[54] Decision on Interlocutory Appeal Concerning Legality of Arrest, *Nikolic* (IT-94-2-AR73), Appeals Chamber, 5 June 2003 [24].

comparatively higher than the injury, if any, caused to the sovereignty of a State by a limited intrusion in its territory, particularly when the intrusion occurs in default of the State's cooperation."[55] This contrasts with cybercrime where, as demonstrated in Chapter 4, there is no such universal recognition and condemnation. As a result, impunity may not pose the same "damage to international justice" that would outweigh a potential intrusion on the host country's sovereignty.

Additionally, the case precedent from the ICTY, which is an international tribunal constituted by the UN Security Council, may not readily extend to when a single country is seeking to lure a cybercriminal. In the Nikolic case, the Trial Chamber repeatedly emphasized, "the relationship between the Tribunal and national jurisdictions is not horizontal, but *vertical*."[56] A pursuing country and host country "function concurrently on an equal level, [so] it is of utmost importance that any exercise of such national jurisdiction be exercised in full respect of other national jurisdictions … The role of the Tribunal, as an enforcement measure under Chapter VII of the UN Charter, is from that perspective, fundamentally different. Consequently, in this vertical context, sovereignty by definition cannot play the same role."[57] In the Dokmanović case, the Trial Chamber also noted the Court's special position as an instrument of the Security Council. Thus, the Trial Chamber explicitly left open the question as to whether a lure (or capture) by a pursuing country would result in a sovereignty violation.[58]

Likewise, the obligation on all states to cooperate with the ICTY means that an extradition treaty is not necessary to render a fugitive. Therefore, an abduction or lure would not circumvent such an agreement. This obligation also means that "a defendant has a right to be free of the process of other national courts while residing in his home country,

[55] Decision on Interlocutory Appeal, *Nikolic* [26].
[56] Decision on Defence Motion, *Nikolic* [76].
[57] Decision on Defence Motion, *Nikolic* [110].
[58] Decision on the Motion for Release, *Mrksić et al.* [77].

but he does not have a right to be free of the ICTY's process."[59] These differences between how war crimes and cybercrimes are prosecuted suggest that higher standards should apply for deploying a unilateral alternative against a cybercrime. To determine those higher standards, we should now look to the literature on conduct that may not constitute a universal crime and that is prosecuted by nation-states rather than international tribunals.

6.3 Terrorism: Self-Defense, Necessity, or an Efficient Breach?

One such crime that satisfies both criteria is terrorism. Nevertheless, legal scholars have asserted that unilateral alternatives may still be permissible here under theories of self-defense, necessity, the failure of host countries to exercise due diligence, and efficient breach. The strict interpretation of self-defense may not apply to cybercrime, which does not entail an armed attack. Yet, the other justifications can be relevant to cybercrime. Indeed, they suggest that unilateral alternatives should only be applied as a last resort in cases posing a significant and imminent harm. They also indicate that the host country should be complicit by failing to cooperate. However, this requirement should be relaxed in cybercrime to account for the challenges of attribution.

While terrorism in the general sense may be universally condemned, countries still disagree as to its definition and the scope of proscribed conduct. As Findlay explains, "not all terrorist acts are anathema to the international community … terrorism as a general matter is perhaps still too controversial in the world community to consider a crime against all humanity."[60] Indeed, only specified terrorist attacks, such as aircraft hijacking, hostage taking, and attacks against internationally protected persons, are subject to universal

[59] Sridhar, "The International Criminal Tribunal for the Former Yugoslavia's Response to the Problem of Transnational Abduction," 356.
[60] Findlay, "Abducting Terrorists Overseas for Trial in the United States: Issues of International and Domestic Law," 42.

jurisdiction. Plus, the Appeals Chamber did not include terrorism in the list of universally condemned offenses that it enumerated in the *Nikolic* case.

Likewise, there are no international tribunals to prosecute terrorism. Instead, the burden falls on national courts, which are reliant on the cooperation of host countries to bring these perpetrators to justice. Therefore, when cooperation has failed, certain pursuing countries have turned to unilateral alternatives. In response, the legal literature has outlined a variety of legal bases for when such tools, namely capture operations, would be permissible. It is important to note that these justifications strictly focus on capturing a terrorist to prosecute in the pursuing country's criminal courts. They do not refer to the US's practice of extraordinary rendition. This tactic began following the September 11th attacks and involved apprehending terrorists for indefinite detention or transfer to other countries for torture.

Similar to war crimes, scholars have first turned to the justification of self-defense for the use of unilateral alternatives in terrorism. Findlay notes that when countries, like Iran, Libya, and Syria, have acted as state sponsors, terrorist attacks can be deemed an armed attack within the meaning of Article 51 of the UN Charter.[61] Therefore, victim countries would be entitled to use force to counter this threat by removing and prosecuting the responsible individuals.

Additionally, Findlay asserts that countries have an inherent right to protect their nationals abroad. He explains that "an attack directed at the nationals of a state may be considered an attack on the state itself and would allow a state to use armed force to protect its nationals from harm."[62] The only condition is that the use of force is necessary and proportionate to that harm.[63] This justification may bring to mind a rescue operation

[61] Findlay, 22.
[62] Findlay, 27.
[63] Findlay, 27–28.

rather than an abduction for criminal prosecution. Yet, Findlay contends that such a capture would be necessary to "prevent future attacks by the particular terrorists involved and deter other terrorists from targeting" the pursuing country's nationals.[64] The use of force involved in a capture would also be far less than the harm of a potential terrorist attack and thus proportionate.

Even more broadly, scholars have acknowledged that countries have a customary right of self-defense, which enables them to use force to protect the lives or property of their nationals. Some scholars argue that this right has been superseded by the conditions on the use of force outlined in the UN Charter. Nevertheless, others posit that, absent an express prohibition in the Charter, this preexisting right survives. Like the previous justification, this logic would permit a capture operation as long as it was necessary and proportionate and the host country was complicit.[65]

These legal arguments are similar to the grounds of necessity, which could be used as a further defense for a unilateral alternative. According to the International Law Commission's (ILC) Articles on the Responsibility of States for Internationally Wrongful Acts, the wrongfulness of an act is precluded if it is "the only way for the State to safeguard an essential interest against a grave and imminent peril."[66] This applies as long as the breach does not "seriously impair an essential interest" of the host country or "of the international community as a whole."[67] The state breaching the obligation also must not have contributed to the condition of necessity. And, the act must conform with peremptory norms of international law, such as the prohibition on the use of force.

Furthermore, legal scholars have affirmed that under customary international law, states have long had an obligation to prosecute and punish criminal offenders who affect

[64] Findlay, 29.
[65] Findlay, 30–31.
[66] "Responsibility of States for Internationally Wrongful Acts."
[67] "Responsibility of States for Internationally Wrongful Acts."

another state or its citizens. Gurulé points to Justice Wilson's ruling in the *Henfield's Case*, which declared that if a country refuses to bring such perpetrators to justice "'it renders itself in some measure an accomplice in the guilt, and becomes responsible for the injury.'"[68] This notion has been repeatedly upheld in international arbitral decisions, such as the *Janes Case*, which found that "the Government is liable for not having measured up to its duty of diligently prosecuting and properly punishing the offender."[69]

As a result, Gurulé argues that a host country's failure of due diligence to prosecute and punish (or extradite) such a perpetrator constitutes an abuse of their territorial sovereignty. This breach of the host country's responsibilities then entitles the victim country to engage in a unilateral alternative to right the wrong and protect their nationals.[70] Abramovsky and Eagle advance a similar argument that the failure of due diligence breaches the sovereignty of the victim country. Therefore, the host country is precluded from later claiming that a unilateral alternative violated their sovereignty.[71] After all, the harm stemmed from the host country providing "sanctuary to alleged offenders."[72]

Even if these legal justifications fail to be compelling, the violation of international law from a unilateral alternative could be considered an efficient breach. This concept, borrowed from contract law, suggests that a breach of the law may be more efficient that following its strictures. In other words, the benefits to the victim country and international community in removing the terrorist and stopping his attacks may exceed any harm done to the host country.[73] A breach would be efficient if certain conditions are met. First, the threat must be imminent, and the opportunity for unilateral action must be fleeting.

---

[68] Gurulé, "Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad," 473.
[69] Janes Case (U.S. v. Mex.), 4 R.LA.A. 82 (1925) [20].
[70] Gurulé, "Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad," 491.
[71] Abramovsky and Eagle, "U.S. Policy in Apprehending Alleged Offenders Abroad," 92.
[72] Abramovsky and Eagle, 92.
[73] Calica, "Self-Help Is the Best Kind: The Efficient Breach Justification for Forcible Abduction of Terrorists," 414.

Second, the host county must be unwilling to extradite or prosecute. Third, the threat to bystanders must be minimal. Fourth, the territorial infringement must be limited. Fifth, the accused must receive humane treatment and a fair trial.[74]

Now, what lessons from these legal justifications advanced for terrorism might apply to cybercrime? On the one hand, terrorism is a violent offense that poses a direct threat to human life. This suggests that higher thresholds should apply to cybercrime, that is if unilateralism is to be advisable at all. Indeed, Gurulé indicates that there should be greater deference to the sovereignty and territorial integrity of host countries for nonviolent crimes.[75] On the other hand, all the above justifications have been advanced for capture operations. These entail a greater intrusion on the sovereignty of the host country and human rights of the accused than a mere lure operation. This suggests that a lower threshold should apply to the use of lures in cybercrime, thus mitigating the nonviolent nature of these offenses.

In addition, the basis for jurisdiction is typically clearer for cybercrime. Since the offenses generally have effects within the territory of the pursuing country, jurisdiction is achieved under the territoriality principle. This contrasts with the terrorist attacks that have traditionally been targeted for unilateral alternatives. Those attacks occurred in a country other than the pursuing country. So, the pursuing country exerted jurisdiction under the passive personality principle if its nationals were targeted, the protective principle if there was an injury to its national interests, or the universality principle if one of those universally condemned terrorist acts was committed.

[74] Calica, 415.
[75] Gurulé, "Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad," 491.

As Calica notes, the "nexus [from the pursuing country] to the act of terrorism is tenuous" in those cases.[76] Indeed, McAlister asserts that "the closer the jurisdictional nexus between the fugitive and the prosecuting state, the more justified a state is in asserting its power over an offender. This suggests a hierarchy of the jurisdictional theories that reflects the crime's connection to the forum state in descending order: territorial, nationality, passive personality, protective, and universal."[77] This difference in jurisdictional basis between cybercrime and terrorism would indicate that unilateral action is more justified for cybercrime, further supporting a lower threshold and mitigating its nonviolent nature.

But, how specifically could the advanced theories pertain to cybercrime? The traditional view of self-defense would not likely apply to the cybercrimes currently subject to criminal prosecution. These frauds, thefts of intellectual property (IP), and data breaches could hardly be considered an armed attack, even if they are state sponsored. Likewise, most cybercrimes do not currently pose a threat to the lives of nationals abroad.

Nevertheless, this may change over time, particularly as cybercriminals target health care systems and critical infrastructure. In fact, such attacks have already led to death. In September 2020, a hospital in Dusseldorf, Germany suffered a ransomware attack, which knocked out their systems. As a result, they had no choice but to begin refusing emergency patients. This meant that a female patient in life-threatening condition was redirected to a hospital 20 miles away. She later passed away due to the delay in treatment.[78] The attack was not intended to result in death. However, a lure operation could be a proportionate and justified response here to protect the lives of nationals

[76] Calica, "Self-Help Is the Best Kind: The Efficient Breach Justification for Forcible Abduction of Terrorists," 407.
[77] McAlister, "The Hydraulic Pressure of Vengeance: United States v. Alvarez-Machain and the Case for a Justifiable Abduction," 513.
[78] Eddy and Perlroth, "Cyber Attack Suspected in German Woman's Death."

abroad. This would be true if the attack had threatened citizens of the pursuing country and the lure was necessary to stop it or future attacks.

Furthermore, the broader right to self-defense to protect the property of a country's nationals could apply now. After all, cybercriminals are pilfering vast sums of money, private data, and IP. For a unilateral alternative to be justified, the pursuing country would need to demonstrate that it was necessary and proportionate and that the host country was complicit. The first component could be satisfied if the cybercrimes were ongoing, cooperation with the host country was not possible, and the perpetrator did not travel on his own. Indeed, as former CCIPS Chief Michael DuBose recalled to me, "in certain cases, [a lure] was almost the only way to have any deterrent impact whatsoever."[79] If the crimes were no longer ongoing or the offender was no longer launching attacks, the lure would not be necessary to defend the property of the pursuing country's nationals. Likewise, if the host country were willing to assist or the perpetrator traveled to more cooperative jurisdictions, the lure would again not be necessary.

The second criterion could be satisfied for significant cybercrimes, measured in terms of the monetary loss, number of individuals victimized, or sensitivity of data stolen. The use of a lure would thus be proportionate since it would entail a minimal intrusion on the sovereignty of the host country and rights of the accused in response to a nonviolent yet highly damaging offense. The risk of causing international strife, however, would not be proportionate to a small-scale or one-off cybercrime.

The third criterion is most clearly satisfied in cases involving state sponsorship or support of cybercrime. Yet, it can also be met in cases where the host country lacks the political will to assist. In that scenario, the host country essentially becomes complicit in the cybercrimes since, for political reasons, they allow them to continue unabated. The

[79] DuBose, interview.

host country therefore abuses its sovereignty by permitting the cybercriminal to use its territory as a base for launching cyberattacks around the world. This is distinct from a scenario where the host country makes a good faith effort to extradite or prosecute but is unsuccessful due to lack of resources or expertise.

Nevertheless, countries should also be able to consider the unique difficulties of attributing cybercrimes. As discussed in Chapter 5, attribution poses less of a challenge in terrorism prosecutions. For example, one prosecutor explained to me that "the advantage in terrorism cases is that if you are going to commit an attack, someone has to emerge."[80] This does not apply to cybercrime where perpetrators can remain hidden behind their computer screens. As a result, law enforcement frequently cannot determine where the cybercriminal is located, let alone his real-world identity.

The self-defense model would preclude using a lure in a case where the host country was unknown, even if the lure was necessary and proportionate. The pursuing country would simply not be able to demonstrate complicity. Yet, Findlay advanced this justification in the late 1980s when information technology was not as ubiquitous as a tool for criminals to conceal their illicit conduct. Therefore, in response to these changes in technology, greater leeway should be afforded such that lure operations can be launched to overcome the attribution challenge. Otherwise, significant harms would continue unabated simply because criminals now have more sophisticated tools at their disposal.

Moving on to the defense of necessity, this could again apply when all other means to bring the perpetrator to justice are exhausted and the lure operation is indeed the only way to safeguard the essential interest. It's important to note that the standard of essential interest does not require the very existence of the state to be in jeopardy.[81] Protecting the

[80] Prosecutor 31, interview, March 15, 2021.
[81] Boed, "State of Necessity as a Justification for Internationally Wrongful Conduct," 15.

property and privacy of its citizens, IP rights of its corporations, and integrity of its financial system could all arguably be considered essential interests. Lures also have spillovers that benefit the international community. They remove cyber threat actors and safeguard international trade and commerce from theft and fraud.

The next component of grave and imminent peril may invoke images of an impending military or nuclear attack. However, international law scholars agree that the bar is not so impossibly high for cyberattacks. The International Group of Experts affirmed in the *Tallinn Manual 2.0* that a grave and imminent peril may include cyberattacks that have a "severe negative impact on a State's security, economy, public health, safety, or environment" as well as "the loss of confidence in the longer term" in banking system or the economy.[82] An example of this could be the cybertheft of IP. As Rowe explains:

> it can erode a country's economy by removing the competitive edge of its private companies, undermining the return on those companies' investments in research and development (which disincentivizes such investments in the future), and transferring large amounts of wealth (in the form of valuable information) to foreign competitor companies who have not made such investments…[83]

The element of imminence can refer to crimes that are either ongoing or "a series of related cyber operations" according to the *Tallinn Manual 2.0*.[84] This condition is likely to be satisfied in many cybercrime prosecutions given the ease for perpetrators to continue their attacks. Indeed, one prosecutor explained to me, "We're dealing with crimes in progress. They're not over. We're not coming in after the fact."[85]

Lures would satisfy this condition not only by arresting the perpetrator behind an ongoing attack. They also enable law enforcement to infiltrate cybercriminal networks and apprehend the kingpins. Such penetration usually requires back-stopped personas. This

[82] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 137, 139.
[83] Rowe, "Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire," 65.
[84] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 139.
[85] Prosecutor 38, interview.

access ordinarily could take years to develop. Meanwhile, the cybercriminal network is continuing to inflict devastating damage on its victims. However, a lure operation can provide an opportunity to clandestinely take over the defendant's online persona, disrupt the network, and "maximize the psychological impact."[86]

This benefit of lures played out in the prosecution of Vietnamese cybercriminal Hieu Minh Ngo. From 2007 to 2013, he operated an online marketplace to sell the personally identifiable information (PII) of 200 million Americans. This conspiracy netted Ngo $2 million and enabled swindlers to file $65 million in fraudulent income tax returns.

During the investigation, agents had discovered the source of the Ngo's compromised information: the credit reporting agency Experian. Posing as a British fraudster, law enforcement contacted Ngo and presented him with a proposition. Join forces or they would cut off his access to the PII. Ngo refused. So, Experian shut down his access, and the undercover agent informed Ngo that he would need to meet with him in person and pay to resume access. But, Ngo refused and simply turned to another source of PII. Law enforcement again identified his source and shut it down. Finally feeling the heat, Ngo agreed to meet in Guam, a little-known US territory where he was arrested.[87]

A federal agent recollected that after arresting Ngo on the lure, "it was a seamless transition except for his flight time. So, we probably had him cooperating within two hours of landing, and then within three hours [we were] back online responding to people."[88] This access enabled law enforcement to smoke out and arrest Ngo's co-conspirators, bringing down the cybercriminal network.

Alternatively, per the *Tallinn Manual 2.0*, imminence can be satisfied when the window of opportunity to address the threat is fleeting.[89] In cybercrime, it can be

[86] Law Enforcement Official 1, interview.
[87] Federal Agent 11, interview, August 22, 2019.
[88] Federal Agent 11.
[89] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 139.

incredibly challenging for investigators to identify and track cybercriminals. The minute these perpetrators suspect law enforcement is on their heels, they can go underground. They can cover their tracks, destroy evidence, and change their online personas with just a few keystrokes. Undercover agents can then lose their line of communication with the offender and the window of opportunity to execute a lure operation.

Despite the above advantages, lure operations take time to plan and execute, especially if the ruse is to be credible. This therefore raises the question of how such an alternative to extradition can really address an imminent threat. After all, there may be a significant delay between when the cybercrime is discovered and when the lure operation is deployed. However, there may be no quicker and less intrusive alternative to stop the ongoing cybercriminal conduct. The host country may not cooperate in prosecuting, extraditing, or informally handing over the defendant. While a capture operation may be faster to carry out, it would entail a much greater intrusion on the sovereignty of the host country and human rights of the accused. Therefore, it would likely fail the next criteria.

Specifically, any action taken on the grounds of necessity must not seriously impair an essential interest of the host country. While a claim can be made that part of the deception of a lure takes place in the host country, this incursion on their sovereignty is minor and bounded. It does not challenge their control over their territory. Nor does it preclude the host country from otherwise enforcing the law in its jurisdiction. It simply stops them from shielding a criminal from prosecution. This differs from a capture operation where agents of the pursuing country unilaterally enter the host country's territory and exercise law enforcement jurisdiction there by arresting one of their citizens.

Moreover, the luring country has done nothing to contribute to the condition of necessity. Even with the best cyber defenses, countries would still fall victim to cybercrime as it is impossible to fully protect against such a rapidly evolving threat. In

fact, "the International Group of Experts agreed that mere failure to take preventive measures to protect a State's cyber infrastructure from harmful cyber operations amounting to 'grave and imminent peril' does not bar measures based on necessity."[90] Finally, a lure would not violate a peremptory norm of international law, particularly since it does not entail the use of force.

The due diligence argument could also apply to certain cybercrime cases. When the host country either protects international cybercriminals or lacks the political will to pursue them, that country fails to meet its international obligations. It fails to make a good faith effort to prosecute and punish the conduct. Its actions thus abuse its sovereignty and infringe on the sovereignty of victim countries by allowing crimes affecting them to continue unabated. As a result, the host country may be estopped from claiming that efforts to bring the perpetrators to justice, such as a lure, violate their sovereignty.

Lastly, the use of a lure operation in a cybercrime prosecution could be considered an efficient breach. The requirement of imminence could be satisfied per the definition from the *Tallinn Manual 2.0*. As also explained above, the opportunity for unilateral action may often be fleeting. Indeed, like Calica argues with respect to terrorism, "a state that hesitates to act … may lose the opportunity to act at all."[91]

Second, the host county must be unwilling to extradite or prosecute. This may occur when the host country lacks political will or supports cybercrimes. Or, there may be insufficient evidence to establish attribution.

Third, lures are an inherently nonviolent alternative that pose a minimal threat to bystanders. They simply seek to deceive the perpetrator into leaving his home country. While there is a possibility the cybercriminal could resist arrest, this risk is minimal.

---

[90] Schmitt, 140.
[91] Calica, "Self-Help Is the Best Kind: The Efficient Breach Justification for Forcible Abduction of Terrorists," 426.

Cybercriminals are not generally violent individuals. Plus, the arrests can be made in a controlled manner, such as while the defendant is passing into the country or at a staged meeting. Law enforcement can easily protect bystanders in either scenario. In fact, the risk of violence posed by a lure operation is no different than arresting a fugitive who is caught while travelling internationally on their own accord.

Fourth, lures present limited, if any, territorial infringement on the host country. According to international tribunals, lures do not violate the sovereignty of the host country since the arrest does not take place there. Legal scholars have further noted that "'actions specifically directed against individuals within the territory of a state do not violate the territorial integrity … of that state.'"[92] Even if you reject these interpretations, a lure only consists of deceiving one of the host country's citizens for a limited period. This is a minor infringement, particularly compared to a capture operation.

Fifth, the accused must receive humane treatment and a fair trial, which can be guaranteed once the defendant arrives in the pursuing country.

Collectively, the above legal justifications for unilateralism in terrorism prosecutions suggest that higher standards exist for offenses that are not universal crimes or prosecuted by international tribunals. Specifically, it must be a last resort, in response to a significant and imminent threat, and a proportionate response. But, how do these criteria apply to crimes that are not necessarily violent or do not pose the same risk to human life as terrorism? Can unilateralism still be justified?

6.4 Drug Trafficking: Analogy to Piracy and Similar Justifications to Terrorism

To answer these questions, I now look to drug trafficking prosecutions, which have relied at times on unilateral alternatives. While violence can often be a consequence of drug trafficking, that is not always the case. It is not an inherent element of these offenses

[92] Quoted in Sadoff, *Bringing International Fugitives to Justice*, 522.

as it is in terrorism. Indeed, over the years, certain drug trafficking organizations, like the Cali cartel, have eschewed violence to fly under the radar of law enforcement.

However, legal scholars have still defended the use of unilateral alternatives to combat this transnational crime. They have adopted similar rationales to terrorism cases based on the failure of host countries to combat criminal threats emanating from their territory. Overall, the criteria for unilateralism in drug trafficking prosecutions reaffirm the conclusions of the last section that these tools should only be used as a last resort in significant cases. Nevertheless, the literature in drug trafficking suggests that such tools are more justified for crimes that are for the personal benefit of the perpetrators.

The logic of permitting unilateralism for drug trafficking has stemmed, at least in part, from the analogy with piracy. Specifically, Fletcher notes that:

> transnational crimes such as piracy and drug trafficking are often best punished by states other than the sovereign nation to which the defendant claims a connection. Such a punishment regime is effective because the crime at issue imposes costs outside the country from which the defendant operates. The second concept which guided piracy law and applies equally to drug trafficking is that some nations are more willing and able to enforce the law than others.[93]

Based on this logic, unilateral action was justified to combat piracy. Given the core similarities, Fletcher asserts that the limited use of unilateral alternatives should be permitted against drug trafficking.[94]

This same analogy can extend to cybercrime, which can satisfy both elements above. The predominant harmful effects occur outside the host country since cybercriminals specifically target their attacks abroad while avoiding domestic victims. Pursuing countries are also often more willing to prosecute these cases, especially when host countries lack the political will to cooperate or sponsor cybercrimes.

---

[93] Fletcher, "Pirates and Smugglers: An Analysis of the Use of Abductions to Bring Drug Traffickers to Trial," 263.
[94] Fletcher, 263–64.

One distinction does emerge between cybercrime and Fletcher's framework for drug trafficking. Fletcher observes that "the cartels exist for the private benefit of the drug traffickers … the sole motive of the drug traffickers is profit."[95] This suggests unilateral alternatives would be more justified for offenses involving personal gain, in Fletcher's view. In drug trafficking, this private benefit predominantly takes the form of significant illicit proceeds. In cybercrime, it may similarly take the form of economic profit. However, it may also include individuals launching cyberattacks as a means of developing their hacking abilities or gaining personal entertainment.

Reminiscent of terrorism, international law scholars have also contended the use of unilateral alternatives is permissible in drug trafficking cases when host countries fail to fulfill their international obligations. Kallenbach argues that "nations have an obligation not to let their citizens engage in criminal activities that affect other nations."[96] So, self-help is justified as long as it is necessary and proportionate. He explains that the first component is satisfied when the host country refuses to cooperate in rendering traffickers.

Plus, "the use of self-help in this instance would not be out of proportion to the serious nature of the violation and the massive threat that the influx of Colombian cocaine poses."[97] This is especially true considering that any use of force from a capture operation, for example, is directed at the drug traffickers themselves rather than the host country.[98]

Cybercrime may similarly satisfy this balancing test given the significant losses that it can generate in terms of stolen funds and IP. The magnitude of the threat is further evidenced in attacks against critical infrastructure. Even if one believes the threat of cybercrime is less than drug trafficking, a lure operation involves a lesser intrusion than a

[95] Fletcher, 239.
[96] Kallenbach, "Plomo O Plata: Irregular Rendition as a Means of Gaining Jurisdiction over Colombian Drug Kingpins," 214.
[97] Kallenbach, 214.
[98] Kallenbach, 214.

capture operation, which is the focus of Kallenbach's analysis. Therefore, a lure could still be considered proportionate.

However, in Kallenbach's example of Colombia and the US, a valid extradition treaty was in place. So, does his justification still hold water even if there is no extradition treaty? Indeed, victim countries of cybercrime like the US lack an extradition treaty with some of the most prolific host countries. McCarthy indicates the self-help justification still applies. When the host country acts irresponsibly and fails to bring the perpetrators to justice, it "should not be able to benefit from international law by shielding narcotics offenders from punishment and frustrating prosecution efforts in other countries."[99] Similar to in terrorism, it therefore cannot protest a unilateral alternative as a violation of its sovereignty.

In addition to these overarching theories, McAlister presents a comprehensive framework for when such alternatives are permissible in drug trafficking cases. The goal of that framework is to ensure that drug traffickers cannot escape into safe havens. At the same time, it seeks to reassure cooperative countries that their territorial sovereignty will not be wantonly violated.[100]

First, there must be a valid jurisdictional principle. As discussed in Chapter 2, countries that have been targeted for cybercrime can exert jurisdiction under the objective territorial principle. According to McAlister, this is the strongest basis for jurisdiction.[101]

Second, it must be a serious crime of international character. In providing a more precise definition of this term, McAlister indicates that those offenses outlawed in international treaties could provide a starting point. For drug trafficking, this condition is

[99] McCarthy, "United States v. Verdugo-Urquidez: Extending the Ker-Frisbie Doctrine to Meet the Modern Challenges to Posed by the International Drug Trade," 1099.
[100] McAlister, "The Hydraulic Pressure of Vengeance: United States v. Alvarez-Machain and the Case for a Justifiable Abduction," 512.
[101] McAlister, 513.

easier to satisfy since the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances has 191 parties. There is no such widely agreed international convention for cybercrime. Nevertheless, the Budapest Convention can provide an adequate starting point. Even though only 66 countries are party to the Convention, 152 countries in total have used it as some guideline or source in developing cybercrime legislation.[102] This demonstrates that it does enjoy sufficiently broad acceptance. Another distinction between cybercrime and drug trafficking is that the latter can entail violence and death. Yet, McAlister notes that an act does not need to result in death to qualify as a significant crime of international character.[103]

Third, the host country must fail to extradite or prosecute. McAlister explains that this can be based on historic tendencies. However, McAlister contends that the duty to prosecute does not commence until the host country is notified of the charges. This may work for drug trafficking since state sponsorship is less of a concern. But, this would be an unreasonable requirement in cybercrime if the host country has an established record of supporting these offenses. As raised in Chapter 4, there is a real risk that host countries will not use such information to prosecute the cybercriminal. Rather, they will use it to tip off or coopt him. This would then eliminate all hope of arresting him since he would know not to fall for a lure and travel abroad.

Fourth, all other methods to secure custody must be exhausted. This could include informal cooperation with the host country. Or, it could include waiting for the perpetrator to travel to another jurisdiction that would assist.

[102] Seger, "Results of Capacity Building and Impact on Legislation."
[103] McAlister, "The Hydraulic Pressure of Vengeance: United States v. Alvarez-Machain and the Case for a Justifiable Abduction," 514.

Fifth, the human rights and due process of the defendant must be respected. According to McAlister, this includes avoiding excessive force or torture, informing the accused of the charges he is facing, and promptly presenting him to a judicial authority.[104]

Finally, there must be compelling evidence. McAlister's rationale is that "it is senseless for a state to violate another state's territorial integrity in pursuit of an individual suspect without compelling evidence of that person's guilt."[105] This may be a reasonable expectation for capture operations in drug trafficking. After all, a capture does not help establish proof of guilt. Plus, prosecutors reported to me that there is no significant attribution challenge in drug trafficking cases. Yet, this does not match the reality for cybercrime cases. As I found in Chapter 4, law enforcement often struggles to definitively establish the identities of cybercriminals, which can be overcome through a lure.

This creates a concern that pursuing countries could wind up luring and prosecuting innocent individuals. Even though lure operations often result in the perpetrator confessing, Stewart highlights that foreign defendants "face greater challenges in defending themselves against criminal charges because they are likely to be unfamiliar with the local language, laws, policies and procedures."[106] Without the proper protections in place, the lured individual may thus feel powerless to assert his innocence, particularly considering the resources at the state's disposal. As a result, there is a real risk that any confession may be erroneous due to a lack of understanding or coercion. Indeed, the lured individual may calculate that it is better to confess and receive a shorter sentence than protest his innocence at trial where the odds may be stacked against him and he could receive a longer prison term.

[104] McAlister, 517.
[105] McAlister, 518.
[106] Stewart, "The Emergent Human Right to Consular Notification, Access and Assistance."

Even if the individual is innocent and does not confess, law enforcement could still vigorously pursue the prosecution, potentially due to embarrassment at having lured the wrong person or out of malice. Therefore, it is important that the defendant be guaranteed a criminal trial with full due process rights in the pursuing country. Such safeguards, such as the right to counsel, would provide him with the ability and resources to mount a rigorous defense and challenge the charges against him. Nevertheless, he will still be at a disadvantage facing a foreign legal system. Stewart explains that this issue has typically been mitigated by notifying the consulate of the defendant's home country, who can then intervene in the process, as well as informing the defendant of his right to consular assistance.[107] This suggests that the same protection should be extended to lured defendants. The due process safeguards of a fair criminal trial combined with consular assistance can then allay any concerns the pursuing country lured the wrong individual, particularly in cases where attribution has not been established in advance.

Overall, these justifications for unilateralism in drug trafficking prosecutions support the use of such tools even when the offense is nonviolent. They also affirm the lessons learned from terrorism cases that these methods should only be applied as a last resort in significant cases. Furthermore, they suggest a new criterion that unilateral alternatives should only be applied for crimes motivated by private gain for the accused.

6.5 An International Framework for the Use of Unilateral Lure Operations in Cybercrime Prosecutions

In this section, I now propose a framework for pursuing countries and the international community to consider in evaluating the use of unilateral lure operations in cybercrime. This framework is informed by the above principles of international law but does not seek to resolve the long-standing debates regarding the permissibility of

[107] Stewart, 439.

unilateral alternatives. Instead, it seeks to balance from a public policy perspective the concerns regarding potential breaches of international law and the human rights of the accused, who is innocent until proven guilty in a court of law where he has access to a reasonable defense, against the interests of justice for victims and need for effective deterrence of cybercrime.

Specifically, it strives to minimize any intrusions on the sovereignty of host countries and any international strife. Even if we accept the view that lures do not violate international law, scholars have noted that reliance on unilateral alternatives may undermine the system of extradition and international law enforcement cooperation by calling into question its utility. This regime plays a vital role in most cross-border investigations, so states must be careful not to jeopardize it.[108] Additionally, the proposed framework assists states in considering when the use of lure operations may interfere with the due process entitlements and human rights of the accused.

At the same time, the framework advises pursuing countries when a lure may be a prudent option to secure custody over the perpetrator, eliminate ongoing threats, infiltrate and take down cybercriminal networks, and provide victims with their day in court.

It is important to note that the framework does not constrain countries from engaging in behavior that may otherwise be permissible under international law. If they deviate from the framework, this does not necessarily mean that their actions are unlawful or impermissible. They simply run a greater risk of generating backlash from elements of the international legal and political community.

Additionally, this framework does not just apply to the US. As explained in the opening to this chapter, nations like Belgium, Germany, and Israel have all deployed lures

[108] Sadoff, *Bringing International Fugitives to Justice*, 590–91.

with at least Israel having done so in a cyber case. Therefore, its recommendations are also intended to guide such countries as they assess when to utilize a unilateral lure.

Nevertheless, the framework does not account for any specific constraints that domestic law or case precedent may place on pursuing countries. For instance, a senior English barrister explained to me, "if there'd ever been a lure or an inducement to come into the jurisdiction, that would be relied on by the person who became the defendant in criminal proceedings in the UK as bad faith, abuse of process. 100 percent. It wouldn't necessarily these days be a guaranteed stay of the prosecution, but it would be a very strong argument in favor of it."[109] As a result, even if all the conditions of the framework are met, a lure may not be acceptable in certain countries.

According to this framework, the use of a unilateral lure operation may generally be advisable when:

First, there is no viable and less intrusive alternative to secure custody over the offender. This may occur when the perpetrator's identity can be established but the host country is uncooperative and the defendant is unlikely to travel. Or, his identity cannot be established, and the lure can help do so. This criterion is in line with the justifications advanced for unilateralism in terrorism and drug trafficking cases. The unilateral alternative must truly be necessary as the only way to bring the perpetrator to justice. Otherwise, the pursuing country would be needlessly intruding on the sovereignty of the host country.

This condition may exist when the host country denies assistance for political reasons, such as a lack of political will or desire to sponsor cybercrime. They may refuse to extradite, informally render, or domestically prosecute the defendant. They would therefore fail to fulfill their international obligations to exercise due diligence in punishing

[109] Senior English Barrister 1, interview.

criminals in their territory who harm other states. In effect, the host country would become complicit in the criminal activity by allowing it to continue unabated, so unilateral action may be acceptable.

Under this framework, the pursuing country would not need to first approach the host country and receive an explicit denial of cooperation. Resorting to unilateralism may be prudent if they can demonstrate a record of the host country repeatedly refusing to cooperate on cybercrime prosecutions. Or, the pursuing country may demonstrate reasonable suspicion that the host country is involved in the cybercrime. This departs somewhat from the justifications advanced in drug trafficking. However, the departure is in recognition of the unique political challenges of cybercrime. Certain host countries would simply tip-off the offender so that they can coopt him for state purposes. This would destroy the pursuing country's chances of laying hands on him and enable him to continue launching devastating attacks.

For the lure to be a necessary last resort, the pursuing country should also consider the accused's likelihood of travelling to a more cooperative jurisdiction. If there is evidence that he may soon travel or if he has a record of frequent international journeys, the pursuing country may be able to simply wait for him to visit a country that will hand him over. Then, the infringements of a lure operation and risk of causing international strife would not be prudent since a viable and less intrusive alternative exists.

To determine if waiting for travel is realistic, the pursuing country should weigh the frequency of travel against the threat's imminence. Let's take the example of a cybercriminal who only travels every few years but is inflicting devastating financial losses. Waiting would not be a viable alternative since there would be a need to swiftly stem the ongoing harm.

Another departure from the justifications for terrorism and drug trafficking cases is necessary here to account for the attribution challenges of cybercrime. Specifically, a lure may be advisable in certain circumstances when the pursuing country cannot definitively identify the perpetrator. If he has routed his attacks through multiple countries, the pursuing country may not know where in the world he is located. Therefore, they cannot approach a specific country for assistance. The only viable alternative would be to smoke him out to the pursuing country or a third country.

Even if the pursuing country has identified where the perpetrator is located, law enforcement may still struggle to "place the hands on the keyboard." It may be difficult to definitively prove attribution in order to succeed on an extradition request or convict at trial. Nevertheless, this scenario does not immediately warrant a turn to unilateralism. The pursuing country could coordinate with the host country on a domestic sting operation or other evidence gathering to establish the defendant's identity. This would preclude the need for any unilateral intrusion on the sovereignty of the host country. Accordingly, if such cooperation is possible, the use of a lure operation would not be prudent. However, if the host country refuses to assist, the pursuing country would once again have no viable alternative but a lure operation to establish attribution and bring the perpetrator to justice. Thus, the lure may be advisable, provided that the remaining criteria are also satisfied.

It is important to note that the question of international travel would not apply to cases where attribution is a challenge. Law enforcement may not know the defendant's real-world identity. So, they may not be able to follow his movements. However, there may be scenarios where law enforcement believes they have identified the perpetrator but cannot yet prove his guilt to a satisfactory standard. In such cases, law enforcement may be able to track him to a friendlier country. Yet, they would still struggle to produce

sufficient evidence of attribution for that country to grant extradition. Hence, the need for a lure would remain.

Second, the case involves an imminent and significant threat. The standard for imminence is based on the definition outlined in the *Tallinn Manual 2.0*. This refers to cybercrimes that are both ongoing as well as when there is a series of related cybercrimes (i.e., a recidivist cybercriminal). A lure would enable law enforcement to not only arrest the perpetrator and stop the attack. It would also allow them to infiltrate the cybercriminal organization, arrest higher-ups, and disrupt the conspiracy.

If the conduct has ceased, the pursuing country has greater flexibility, which means that a lure would not be necessary and thus not advisable. For example, the pursuing country could wait for the cybercriminal to slip up and travel. Political tides in the host country may change in favor of cooperation. In the meantime, the perpetrator's freedom would not pose a threat to the pursuing country.

Likewise, the cybercrime should be significant. This can be determined by following a similar approach as the International Criminal Court in assessing the gravity of cases. It considers quantitative factors (e.g., number of victims, amount of loss) as well as qualitative criteria related to the nature, scale, and manner of commission of the crimes; impact on victims; and the extent of that defendant's participation.[110]

By only focusing on cybercrimes that pass this threshold of significance, pursuing countries will ensure that the lure operation is a proportionate response to the offense. Even though lures involve a minor infringement on the sovereignty of the host country and rights of the accused, they still risk causing international strife or undermining the

[110] Hendry, "Determining Whether a Case Has Sufficient Gravity to Be Admissible at the International Criminal Court (ICC)."

extradition system. Therefore, their use in a case involving an insignificant offense would be disproportionate and more likely to generate international backlash.

Third, the crime is suspected to be motivated by private gain for the accused. As discussed in the preceding literature, unilateralism was in part justified for drug trafficking cases since these crimes were committed for the private benefit of the defendants. This suggest that a similar condition should apply for cybercrime. To determine whether a crime is for personal gain, pursuing countries should consider "the motivation, context, methods, and proportionality of the crime to its objectives."[111]

In the context of cybercrime, private benefit may manifest as economic profit, personal learning by developing or practicing one's hacking abilities, or personal entertainment. For example, a cybercriminal may launch a distributed denial of service attack, which overloads a server with excess traffic to cause a website or the targeted organization's computer systems to crash. Oftentimes, these attacks do not bring any financial benefit to the perpetrator. Rather, they may be launched since the offenders have fun engaging in online vandalism. In such a case, the cybercriminals' actions would be motivated by personal gain (entertainment) and thus qualify for a lure operation, provided the remaining conditions of the framework are met.

This criterion would correspondingly advise against using a lure operation for cybercrimes "committed for a political purpose or inspired by a political motive."[112] Such offenses could be directed at the government, such as treason, sedition, or espionage. They could also manifest as common crimes against private interests that seek to advance a political agenda. Indeed, as public discourse increasingly moves online, there is a valid fear that certain countries could use lure operations to prosecute political activity under the

[111] "Guidelines on International Protection No. 5: Application of the Exclusion Clauses: Article 1F of the 1951 Convention Relating to the Status of Refugees," 5.
[112] Law and Martin, "Political Offence."

guise of cybercrime. For example, as discussed in Chapter 4, Russia and China have championed a new UN cybercrime treaty. Their proposal is based on a model of information control rather than crime prevention, which has alarmed international human rights groups.[113]

This limitation on the use of lures would ensure that defendants receive roughly the same procedural protection that they would have received through a formal extradition. Indeed, many treaties expressly prohibit extradition for political offenses although interpretation of that term is generally left to the courts. Some countries, such as the UK, have more recently passed domestic legislation removing the political offense exception to extradition. Other countries, such as the US, have adopted a narrow view of political offenses as generally those acts "committed by a member of a group that was part of a 'temporally and spatially limited' political conflict, uprising, or disturbance 'related to the struggle of individuals to alter or abolish the existing government in their country' or to seek political asylum from governmental oppression."[114]

However, the US approach may unduly deny protection to conduct that was motivated by political objectives simply because it was not part of a defined political conflict or uprising or because the goal was not to alter or abolish the government. As a result, countries, such as those in continental Europe, have adopted a broader view. They include any act that is driven by politics as long as the offense is "proximately related" to the political objective and the political component "predominates over or is proportionally greater compared with [any] common crime dimension."[115]

A key objective of this framework is to advise countries when the use of lure operations may generate international backlash. If pursuing countries were to apply such a

[113] "Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online."
[114] Sadoff, *Bringing International Fugitives to Justice*, 207.
[115] Sadoff, 207.

narrow exclusion of political offenses like that adopted by the US, they could wind up luring cybercriminals for conduct that at least some elements of the international community consider to be genuine political activity. This, in turn, could generate significant international controversy and undermine the legitimacy of the lure operation. Therefore, it would be most prudent for pursuing countries to adopt a broader exclusion and only focus on luring cybercriminals motivated by private gain.

There is a risk though that cybercriminals could begin also engaging in crimes that are motivated by political goals rather than personal gain to escape justice. This framework would advise against using a lure to prosecute them for such political offenses. However, a lure may still be prudent for their cybercrimes that are for private benefit and satisfy the other conditions of this framework.

The exclusion of political offenses also raises questions as cyberattacks turn violent and may lead to bodily harm. Should lure operations still be avoided for such crimes? The international community has increasingly limited the application of the political offense exception to violent acts, particularly with respect to terrorism. The underlying logic here is that the use of violence is "wholly disproportionate to any political objective."[116] Hence, such acts are considered predominantly common crimes. Indeed, many international and regional counterterrorism conventions do not include a political offense exception. Since violent political acts would not generally be shielded from extradition, the use of a lure operation for such a crime would be less likely to generate international backlash. This therefore suggests that a lure may still be prudent for a cyberattack resulting in bodily harm, even if the offense was politically motivated.

[116] "Guidelines on International Protection No. 5: Application of the Exclusion Clauses: Article 1F of the 1951 Convention Relating to the Status of Refugees," para. 15.

Another implication of this element of the framework is that lure operations should not target a state official for acts done in an official capacity. One of the greatest challenges of cybercrime is the blended nature of this threat. Oftentimes, seemingly commercial cyberattacks were actually carried out by state actors for the benefit of their government rather than for their personal benefit. Deploying lure operations in those cases raises concerns related to functional immunity (*ratione materiae*). According to the *Tallinn Manual 2.0*, international law generally holds that state officials enjoy immunity from criminal prosecution in foreign courts for acts done in an official capacity.[117]

Nevertheless, the US has still indicted state officials for cybercrimes that it alleges these individuals perpetrated in their official capacity. The US asserts there is a territorial exception to functional immunity. In other words, the crimes take place in the US since the harm is felt there, and there is no immunity for criminal acts that take place within the territory of the country exercising jurisdiction.[118]

Yet, if territoriality is used as the basis for stripping immunity, other countries could apply the same theory to lure and prosecute any military and intelligence officer for traditional cyberespionage. After all, the effects of such actions occur in the targeted countries' territory. One federal prosecutor explained to me that the US is not concerned by this risk since state sponsors already engage in this type of behavior. In fact, Russia currently issues Red Notices for the arrest of US officials. The prosecutor highlighted that these countries "use power whenever it suits them, so they are not going to be emboldened just because the US starts prosecuting their officials."[119] Additionally, US state actors are not suspected to engage in commercial cybertheft, so their actions should be covered under the political offense exception. However, they could still be arrested if they travel

[117] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 72.
[118] Prosecutor 4, interview, March 31, 2021.
[119] Prosecutor 4.

directly to the indicting country or to a country that does not have a political offense exception in its extradition treaty with the indicting country.

Overall, the US position here risks legitimizing other countries' efforts to prosecute state actors and undermining international stability, particularly if it permits governments to constantly lure each other's officials. This may thereby set dangerous precedent of state practice for the development of customary international law.

While cyberespionage exists on a spectrum and distinctions could be drawn between political and commercial activity, opinions differ as to where the line falls on that spectrum. Plus, international norms are still nascent in this area. Therefore, under this framework, it would be most prudent to avoid lure operations against state officials for cybercrimes committed in an official capacity. It could still be advisable to use lures for cybercrimes that state officials commit for their private or personal gain. It is important to note that this recommendation may change over time. Norms may become further entrenched, and lines may become clearer.

Countries like the US may also decide to assume the risk of backlash from elements of the international legal and political community. They may still decide to lure state actors to prosecute them for their official acts. As a practical matter, state sponsors often explicitly deny their involvement with the indicted cybercrimes. This allows the pursuing state more credibility in proceeding with unilateralism against perpetrators of commercial offenses. Indeed, after the US indicted three Chinese People's Liberation Army officers for cyber IP theft, the Chinese Ministry of Foreign Affairs declared, "the Chinese government, the Chinese military and their relevant personnel have never engaged or participated in cyber theft of trade secrets."[120] However, if the pursuing

[120] "China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel."

country deploys a lure and then alleges that the defendant's acts were on behalf of the state, this could be counter-productive to the international acceptance of unilateralism.

Fourth, the lure does not engage in entrapment or coercion. This serves to preserve the defendant's due process rights. If he were the subject of a domestic investigation, he would generally be protected against entrapment. Therefore, that safeguard should not evaporate merely since he is lured from another country. This means that law enforcement should not unduly urge, harass, or coerce the defendant to commit any cybercrimes in the pursuing country's jurisdiction. However, they may launch an undercover operation to merely offer him an opportunity to engage in cybercrimes or advance an ongoing conspiracy. Law enforcement may then charge him for any criminal acts committed during the lure in response to those opportunities.

It is important to draw this line since pursuing countries could illicitly deploy lures to persecute political enemies or undermine the cyber talent of rival countries by entrapping these individuals. The targets might have never broken the law but for the government's pressure, so such a lure would infringe upon their rights. Moreover, pursuing countries should be using lure operations to combat crime, not create it. This suggests that it would not be prudent to solely charge defendants for crimes committed during the lure. In other words, there should be an underlying pre-existing cybercrime.

In addition, the lure should not coerce the defendant by limiting his freedom of choice to travel to the lure destination. Such coercion could take the form of threatening him or his loved ones. For instance, Chinese agents have threatened and even arrested the relatives of overseas targets to compel those individuals to return to China and face criminal charges.[121] Such law enforcement action would be ill-advised. As the ICTY ruled

[121] Landay, "China Coerces Hundreds of Chinese-Born Critics in U.S. to Return Home, FBI Chief Says."

in *Dokmanović*, the permissibility of lures stems from their voluntary nature and the ability of the defendant to cancel his travel plans at any time prior to arrest.

If the accused were forced to travel, it would undermine his free will and infringe upon his rights. It could also mean that the deprivation of his liberty took place in the host country. Based on the *Dokmanović* ruling, deprivation of liberty occurs when the perpetrator knows that he is no longer free. This could occur if he knew he had no real choice but to travel to a country where he would be arrested. As a result, there would be a greater infringement on the sovereignty of the host country since the pursuing country would effectively be depriving the offender of his liberty and exercising law enforcement jurisdiction in the host country. The only part missing until the perpetrator arrived in the pursuing country would be the physical handcuffs.

Fifth, the accused is guaranteed due process and a fair criminal trial upon arrival in the pursuing country. Such a trial should be public, timely, governed by procedures established in law, and adjudicated by a competent and impartial authority. The defendant should be informed of the charges against him, presumed innocent until proven guilty, and not compelled to testify against himself or confess guilt (e.g., through torture). He should also have a right to access an interpreter, challenge the charges, critically examine any evidence against him, present exculpatory witnesses, and appeal any verdict. Furthermore, the defendant should be entitled to competent and independent legal counsel of his choosing and the appointment of counsel if he cannot afford representation on his own. Finally, he should be protected from *ex post facto* laws.[122]

These provisions will ensure that the cybercriminal's due process rights under international law are fully protected despite custody over him being secured through

[122] This list of due process rights is based on the International Covenant on Civil and Political Rights as well as Bassiouni's review of ten international and regional human rights instruments and 139 national constitutions in Bassiouni, "Human Rights in the Context of Criminal Justice: Identifying International Procedural Protections and Equivalent Protections in National Constitutions."

trickery outside the extradition process. Such safeguards are particularly important for lure cases in cybercrime since compelling evidence of guilt may not be established prior to the operation. Therefore, there is a risk that the pursuing country lured an innocent individual, who must have a fair and equal opportunity to defend himself.

Even if all these procedural protections exist on paper, there is no guarantee that they will be properly implemented in practice. Plus, as noted earlier, defendants are at an inherent disadvantage when they confront a foreign judicial system. Nevertheless, an analogy can be drawn between the situation of a lured defendant and a foreign national who is arrested abroad while, for example, visiting for work or pleasure. Both have travelled voluntarily to the arresting country. Both could be wrongly accused. And both confront the same disadvantages in facing an unknown legal system.

This concern has traditionally been remedied by notifying the consulate of the defendant's home country and informing him of his right to consular assistance. Stewart elaborates, "Allowing the relevant [consular] authorities to contact [the accused] and provide assistance serves as a protection against such risks – by 'levelling the playing field' and helping to ensure fair treatment."[123] These consular authorities can explain the local criminal justice system, contact friends and family, provide a list of local attorneys, and visit the defendant in prison.

In fact, the defendant's home country may be more likely to intervene when he is arrested outside an extradition request. During an extradition, the home country has an opportunity to vet the charges and conditions the defendant is likely to experience in the pursuing country. So, once extradition is granted, the home country may take more of a back seat approach. However, without such vetting, they may adopt a more active or interested role to ensure fair treatment. Indeed, as seen in the previous chapters, this

[123] Stewart, "The Emergent Human Right to Consular Notification, Access and Assistance," 439.

frequently occurs with respect to Russian cybercriminals who are arrested outside of Russia. The highest levels of the government and embassy protest the apprehension and participate in the court proceedings.

Based on the above due process benefits, any lured cybercriminal should thus be informed of his right to consular assistance, and his home country's consulate should be notified at the time of arrest. Notification earlier in the process, such as when the lure operation is launched, runs a risk of the home country tipping off the cybercriminal and foiling the lure. This is especially likely for countries that enable or sponsor cybercrimes.

Overall, the six criteria of this framework have been drafted broadly to reflect the case-specific nature of lure operations and the wide variation within cybercrime. One cannot offer so detailed guidance as to say, for example, that a lure operation would be prudent only for cybercrimes involving a loss of at least $100 million. That may exclude an equally serious data breach that pilfered the personal information of 100 million citizens but resulted in minimal direct financial harm. This generality raises concerns though that pursuing countries could stretch the criteria to use lures in an ill-advised manner that interferes with the rights of the defendant or sovereignty of the host country.

Nevertheless, this framework must rely on the voluntary commitments of pursuing countries and self-policing. In fact, countries have an incentive to follow the framework to minimize the likelihood of generating international backlash. As Calica explains with respect to capture operations, "fear of foreign retaliation and of eroding international institutions and peace provides a check on states."[124] Countries are further incentivized to follow the framework since it may encourage reciprocity. This would then protect their citizens from questionable lures by other countries. While this framework cannot

[124] Calica, "Self-Help Is the Best Kind: The Efficient Breach Justification for Forcible Abduction of Terrorists," 414.

overcome the core enforcement challenges of international law and norms, partial or imperfect compliance is still preferable to the status quo. If the framework guides pursuing countries in deploying lures more prudently, then it has merits.

Likewise, if the pursuing country fails to satisfy the above criteria and contravenes international law in the process, the defendant could challenge his arrest in the pursuing country's courts as an abuse of process. The court could issue a stay of proceedings, and the defendant could be returned to his home country. The risk of that outcome would further deter pursuing countries since it would defeat the purpose of the lure. Granted, this approach may not work with all pursuing countries. For example, US courts have been reluctant to question how custody over defendants has been secured, even if it may appear to violate international law, and have left this for the executive branch to consider.[125]

The host country could also lodge a complaint with the UN. After all, Calica notes that the UN "has historically been the institution of choice for aggrieved nations following forcible abductions … By resolution, the UN can demand that the breaching party pay reparations, impose trade sanctions, or inflict reputational loss."[126] While this approach may still not deter the US or countries less concerned with their international reputation, the humiliation of such a public rebuke could discourage some pursuing countries from engaging in questionable lure operations.

To further examine the robustness of this framework, I applied its criteria to the case studies of US cybercrime prosecutions involving unilateral lure operations. The results are reported in Table 2 at the end of this chapter. I first considered whether there were no viable and less intrusive methods to secure custody. This condition was most clearly satisfied in the Ivanov and Gorshkov and Dolan and Butu cases. In the former,

[125] *United States v. Alvarez-Machain*, 504 U.S. 655, 669 (1992).
[126] Calica, "Self-Help Is the Best Kind: The Efficient Breach Justification for Forcible Abduction of Terrorists," 417.

requests for assistance from Russia in closely related cases went unanswered. In the latter, Romania explicitly refused to cooperate. Plus, in both, the defendants did not have a reliable record of international travel.

This question was less clear-cut in the Klopov, Li, and Ngo cases. Even though the perpetrators did not travel, the host country was never approached for cooperation. Yet, for the first two defendants, Russia and China had an established history of not assisting on cyber cases and even protecting such defendants. For the Ngo case, corruption in the host country similarly precluded approaching them for assistance.[127]

The one borderline case with respect to this criterion was the Nemeth prosecution. While federal agents indicated that attribution was the challenge, he had provided the undercover investigators with his Hungarian passport. So, how could they legitimately claim they did not know his identity? By probing further on these assertions, I learned that the real difficulty stemmed from determining where he was located. Although he had a Hungarian passport, he could travel anywhere within the Schengen Zone without generating records of his location and could launch his attacks remotely. Therefore, US authorities would not know which country to approach for extradition and needed a lure to smoke him out.

With respect to the second condition, all the cases involved continuing crimes, demonstrating the imminence of the threat. However, the degree of harm varied significantly between the prosecutions. On one end of the spectrum, the Ngo and Li cases posed the clearest threat since Ngo had stolen the PII of 200 million Americans and Li was selling software with sensitive national security applications, causing over $100 million in losses. Dolan and Butu had also victimized over 800 businesses and were targeting dozens of new ones daily. While it may not seem significant by today's

[127] Federal Agent 11, interview, September 16, 2020.

standards, Ivanov and Gorshkov caused over $28 million in losses, which was "unprecedented" at the time.[128]

This question becomes less clear again for the Nemeth prosecution. The direct losses to Marriott of $1 million would not have justified a lure under this framework. But, this does not account for the potential losses to Marriott if Nemeth had released the stolen proprietary data, which are unknown. Therefore, it is unclear whether the threat was significant enough for a lure operation to be prudent here. Similarly, in the Klopov case, the only real losses were $1.5 million since the additional attempted thefts had been successfully thwarted. Klopov would have then failed to constitute a significant threat, and a lure would have been inadvisable under this framework.

Each of these six cybercrimes were motivated by financial profit for the perpetrators, so they would have squarely met the third condition. Even though law enforcement considered that Li could be working for the Chinese state, they ultimately found no evidence connecting him to the government. Rather, the evidence suggested that he was working for his own economic benefit.

Furthermore, none of the cases involved entrapment or coercion. In the Ivanov and Gorshkov, Nemeth, and Dolan and Butu cases, the lure did not involve the defendants committing any further cybercrimes. It merely consisted of a job interview or honeypot scheme. The Klopov, Ngo, and Li cases could present concerns of entrapment since the defendants were lured by undercover agents posing as co-conspirators. Nevertheless, law enforcement did not induce them to commit their crimes. They simply provided an opportunity to grow their existing cybercriminal conspiracies.

Finally, all the defendants were guaranteed the full due process protections of a US criminal trial. They were afforded the right to legal counsel. Some were appointed a public

[128] "Russian Man Sentenced for Hacking into Computers in the United States."

defender while others opted to hire their own attorney. For example, Nemeth was represented by an experienced federal public defender. However, his family also hired an attorney from Hungary who travelled to Baltimore and was permitted to participate in plea negotiations and meet privately with Nemeth.[129] Likewise, Klopov was at first assigned a public defender for his arraignment, but then hired a private attorney who has handled multiple cases of foreign nationals extradited to the US for cybercrimes and enjoys a positive reputation among such defendants.[130] Li also was originally represented by a federal public defender but elected to retain a private attorney for his plea negotiations.[131] Moreover, in each of the cases, the lured cybercriminals were offered an interpreter at all court appearances and meetings with prosecutors, and law enforcement provided proper consular notification.

While my framework may appear to be largely in line with the US approach, this analysis indicates that not all US prosecutions would pass its benchmarks. Indeed, a lure operation would not have been prudent in the Klopov case. Similarly, depending on the potential losses to Marriott if the stolen data had been released, a lure may not have been advisable in the Nemeth case either. Since both lures were deployed as a last resort, this suggests that my framework may allow certain cybercriminals to escape prosecution. Nevertheless, this should be less of a concern in cases like these where the crimes do not entail substantial losses and law enforcement may have other means to prevent the harm. The potential international strife that a lure operation could cause would thus override the need to arrest a small-scale cybercriminal.

Several policy lessons can also be learned from the cases that may not have passed this framework. Neither the Klopov nor Nemeth prosecution went through the OIA review

[129] Prosecutor 29, interview, August 13, 2019.
[130] Law Enforcement Official 3, interview, June 7, 2021.
[131] Hall, *CRACK99: The Takedown of a $100 Million Chinese Software Pirate*, 239.

process. The former was a state rather than federal case, and the latter was not classified as a lure since the defendant selected the destination. This suggests that pursuing countries, particularly those with a federal system of government, may wish to adopt a common approval process to ensure lure operations are utilized responsibly. This would minimize diverging approaches among law enforcement agencies as well as between local and national authorities. Indeed, local law enforcement may not have as holistic of an understanding of international politics and the potential ramifications of a lure operation as the federal government. Therefore, without proper oversight, they could deploy such tools recklessly.

Pursuing countries may also wish to ensure they provide clear guidance on the principles that apply to lure operations. Such guidance should be written in a way to mitigate potential loopholes, particularly with respect to the definition of a lure operation. It should not matter whether the defendant selected the travel destination. After all, he would not have been travelling but for the pursuing country's offer or enticement, regardless of who selected the location.

6.6 Concluding Remarks

An effective response to global threats depends on international cooperation. It depends on each country agreeing to forsake the unilateral pursuit of its own interests. Indeed, an international system characterized by rampant unilateralism could soon descend into a dog-eat-dog world of chaos.

At first glance, cybercrime would appear to forestall this outcome. Through the Budapest Convention and its worldwide ripple effect, countries came together to outlaw cybercrime and facilitate mutual legal assistance. Yet, the challenges of securing custody over cybercriminals abroad remain intractable. Politics and the evidentiary difficulties of cybercrime have impeded justice. As a result, the need for unilateralism appears to be here

to stay. If this is the case, there must be some international framework to assist countries and the international community in assessing when such tools may be prudent. Otherwise, unilateralism may run amok, trampling on the sovereignty of host countries and human rights of the accused.

To devise such a framework, I first looked to the safeguards that the US has implemented for its use of unilateral lure operations to determine what, if any, lessons could be learned. I discovered that the US has adopted a multi-step approval process with several criteria that must be satisfied. Specifically, lures are only to be used as a last resort in the most significant cases. They cannot entrap or coerce the accused. And, lures are only applied for criminal conduct, not to prosecute traditional espionage. Additionally, the defendant still receives all the due process protections of a US criminal trial. However, I learned that in the past, USDOJ narrowly interpreted the definition of a lure, allowing cases to escape the approval process. Any new framework should take care to avoid creating such a loophole.

I then looked to the experience of three other crimes where unilateral alternatives have been applied: war crimes, terrorism, and drug trafficking. I sought to determine how the justifications for unilateralism with respect to those offenses could apply to cybercrime. For war crimes, the ICTY has ruled that lures do not violate the sovereignty of the host country or rights of the defendant since he travels voluntarily. The ICTY has even found that capture operations would not provide grounds for setting aside jurisdiction as long as there is no inhumane treatment or torture of the accused. Nevertheless, these cases are different than cybercrimes. They are universally condemned offenses prosecuted by an instrument of the UN Security Council. Therefore, these precedents can only serve as a baseline, and greater safeguards should exist for cybercrime.

Next, I turned to conduct that may not constitute a universal crime and is not prosecuted by international tribunals: terrorism. Legal scholars have advanced several justifications for unilateral alternatives here, including self-defense, necessity, the failure of host countries to exercise due diligence, and efficient breach. Since cybercrime is not typically violent and thus not an armed attack, the strict view of self-defense would not apply. However, the broader conception of self-defense to protect the property of a country's nationals as well as the other justifications remain relevant.

Synthesizing these legal theories suggests that unilateral alternatives should only be applied as a proportionate last resort to combat a significant and imminent harm. The host country should also be complicit. Nevertheless, that last requirement should be relaxed in cybercrime cases to address the attribution challenge. Otherwise, pursuing countries would lose an important tool to stem ongoing harms when they cannot locate or identify the perpetrator but can lure him.

Even though drug trafficking is not necessarily a violent crime, similar justifications for unilateralism have been advanced. When the host country fails to exercise due diligence in addressing criminal threats emanating from its territory, a unilateral response is permissible. It simply must be necessary and proportionate. Indeed, the criteria that legal scholars have advanced for unilateralism in drug trafficking cases reaffirm that they should only be used as a last resort in significant cases. They also add a new consideration that unilateralism is justified, in part, since drug trafficking is for the private benefit of the perpetrators.

Considering these examples and the findings of this dissertation, I conclude by proposing an international framework that outlines the baseline standards for when the use of unilateral lure operations in cybercrime may be prudent. Specifically, 1) there are no viable and less intrusive alternatives; 2) there is a significant and imminent threat, 3) the

crime is suspected to be motivated by private gain for the accused; 4) law enforcement does not engage in entrapment or coercion; and 5) the accused is guaranteed a fair trial with full due process protections.

By adhering to the recommendations of this framework, the US and other countries that follow suit can overcome the hurdles of bringing international cybercriminals to justice. And they can do so in a manner that is less likely to provoke criticism from elements of the international legal and political community.

Table 2: Applying the International Framework to US Cybercrime Prosecutions Involving Lure Operations

Criteria	*USA v. Gorshkov, et al (2000)*	*NY v. Klopov (2007)*	*USA v. Nemeth (2011)*	*USA v. Oprea, et al (2011)*	*USA v. Li, et al (2011)*	*USA v. Ngo (2013)*
No viable and less intrusive alternative	Yes – host country would not cooperate and no reliable record of travel, especially considering ongoing and escalating threat.	Yes – could not definitively establish attribution and host country unlikely to cooperate.	Yes – could not determine where he was located and could not wait for travel considering the ongoing threat.	Yes – host country refused to cooperate and not possible to track travel.	Yes – host country refused to cooperate and did not travel.	Yes – corruption in host country precluded cooperation and did not travel.
Significant and imminent threat	Yes – continuing to launch attacks against internet service providers, already caused an estimated $28 million in losses and stole at least 56,000 credit cards. Judge described case as "unprecedented … criminal enterprise."	**NO** – posed an imminent but NOT a significant threat. His crimes only involved $1.5 million in losses from a small number of victims. While he tried to steal a further $7 million, these attempts were all thwarted by the victims' banks.	Unclear – direct losses likely would not justify lure, but unclear what harm he could have caused if he released the data. Marriott believed it would cause "irreparable damage."	Yes – hacked over 800 businesses in four months, stole payment card information of over 6,000 people, and attempting to hack dozens of merchants daily.	Yes – was continually selling cracked software worth over $100 million with critical national security applications.	Yes – had stolen the PII of 200 million Americans and was seeking to steal further data.
Motivated by private gain for the accused	Yes – theft of card details, extortion, fraud	Yes – identity theft and fraud	Yes – theft of data and extortion	Yes – theft of payment card information	Yes – theft of intellectual property	Yes – theft of PII and identity fraud
No entrapment or coercion	Yes – lure solely consisted of a job interview.	Yes – in furtherance of existing conspiracy.	Yes – lure solely consisted of a job interview.	Yes – lure not related to the charged conduct.	Yes – in furtherance of existing conspiracy.	Yes – in furtherance of existing conspiracy.
Full and fair trial	Yes	Yes	Yes	Yes	Yes	Yes

7. CONCLUSION

This dissertation began with the story of Evgeniy Bogachev, founder and leader of the Gameover Zeus botnet and CryptoLocker ransomware. In many ways, his case represents cybercrime's both evolution and continuity over the past two decades. The most pernicious cybercrimes are no longer attacks like the Ivanov and Gorshkov case from the early 2000s, where the perpetrators were focused on hacking into companies to steal credit card information. Indeed, the potential loss of $28 million that was considered "unprecedented" back then seems quaint by today's standards.[1] Rather, the most pernicious cybercrimes are now ransomware attacks like CryptoLocker. Such schemes are estimated to generate global damages of $20 billion by the end of 2021, which is a 57-fold increase from 2015 and demonstrates the exponential growth of cybercrime.[2]

Despite these changes in tactics, many of the core challenges to combatting cybercrime have remained the same. For example, the perpetrators tend to remain indefinitely in countries where they will not be extradited or prosecuted. Some countries take this a step further, actively guarding cybercriminals from foreign law enforcement. Just as Ivanov and Gorshkov believed the Russian government would coopt them rather than hand them over to the Americans, Bogachev appeared to have become a Russian intelligence operative. He was using his criminal skills to accomplish state objectives.[3] Considering these persistent obstacles, it is unsurprising that so few international cybercriminals are ever brought to justice.

This dissertation has sought to shed light on one aspect of that enforcement gap in cybercrime: the difficulty of securing custody over the offender. Even though countries have strived to create a system of international cooperation through extradition, it has

[1] "Russian Man Sentenced for Hacking into Computers in the United States."
[2] Morgan, "Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021."
[3] Carlin, *Dawn of the Code War*, 292, 297.

often failed to result in the apprehension of cybercriminals. This study has endeavored to explore why and understand how this may influence states' use of alternative mechanisms to secure custody. Specifically, this research has strived to answer two core questions:

1. *Are pursuing countries more likely to apply unilateral alternatives over extradition and quasi-extradition in prosecutions of cybercrime than other transnational crimes?*
2. *What factors influence the use of unilateral alternatives to extradition in cybercrime cases?*

In this chapter, I will revisit the core predictions, methodology, and findings of this study. I will then explore the generalizability of the conclusions beyond the United States, examine the implications of the results for international law and policy, and identify several directions for future research.

7.1 Summary of Key Findings

A core difficulty of studying a topic as novel and evolving as cybercrime is the lack of well-established literature from which to draw. Although extradition regimes have existed for centuries, there have been no prior attempts to explore the successes and failures of this system as it relates to cybercrime. Is cybercrime a type of old wine in new bottles, facing similar difficulties as other types of transnational crime? Or is it something new, suffering from unique challenges in bringing perpetrators to justice? Filling that lacuna in the literature marks the first contribution of this dissertation.

In Chapter 2, I surveyed existing scholarship, which revealed the political and procedural obstacles that generally plague the systems of extradition and transnational criminal law. This has curtailed their effectiveness in facilitating the rendition of international fugitives. As a result, countries may face a quandary: should they abandon

the case or turn to alternatives to extraditions? Such tools include quasi-extradition and unilateral action.

Discussions of these alternative approaches have focused on their legality under both US domestic and international law. While US Supreme Court precedent has made clear their permissibility under domestic law, this remains an open question with respect to international law. Scholars debate whether unilateral alternatives violate the sovereignty of the host country or infringe upon the human rights of the accused. Some scholars have even advanced arguments outlining when these tools may be justified for specific types of transnational crimes. Nevertheless, there have been no such efforts to determine when unilateral alternatives may be justified in cybercrime cases. Nor have there been any attempts to examine the causal factors that influence when states deploy these tools.

To address these further lacunae, I applied the existing literature to predict how the use of extradition and its alternatives may differ, if at all, for cybercrime. I posit that cybercrime faces unique challenges related to the facts of the case, applicable laws, and political considerations. Specifically, the remote nature of cybercrime means that perpetrators may never enter the victim country's territory. So, pursuing countries will need to rely more heavily on extradition and its alternatives. Yet, the ability for cybercriminals to target countless victims in multiple countries may generate jurisdictional conflicts, leading countries to resort to unilateralism to preempt each other.

Additionally, a lack of legal harmonization between countries on cybercrime may block extradition due to dual criminality requirements. Likewise, cybercriminals, especially those who are state sponsored, may argue that their conduct constitutes a political offense. This would again preclude extradition. Furthermore, countries may lack the political will to cooperate in cyber cases since the victims are typically located abroad and there are little to no harmful domestic consequences. Hence, countries have little

incentive to expend resources in handing over perpetrators. Even worse, certain countries may view cybercriminals as potential assets and therefore seek to protect them from prosecution abroad. These challenges collectively led me to the prediction that pursuing states are more likely to employ unilateral alternatives over extradition and quasi-extradition in prosecutions of cybercrime than other transnational crimes.

In Chapter 3, I outlined my approach to answering the core research questions and testing this hypothesis. Given the US's leading role in prosecuting cross-border cybercrime, I focused my analysis there. Ideally, I would have compiled a dataset of prosecutions of transnational crimes and the methods used to secure custody over each defendant and run a regression. However, the US government does not maintain such data over how defendants are brought to trial. As a result, I adopted a qualitative approach consisting of comparative elite interviews and case studies.

This research strategy presented both strengths and weaknesses. Primarily, it enabled me to hear directly from the law enforcement officials combatting cybercrime and deploying alternatives to extradition. This provided the thick descriptions that cannot be gleaned from quantitative analysis alone. Indeed, such rich explanations are particularly valuable for studying areas that lack well-developed theory. This permitted me to both test my theory outlined above as well as identify new causal variables of interest.

Nevertheless, qualitative data cannot provide definitive answers to the research questions in the same way a quantitative analysis could have. The recollections of interviewees may be skewed by the limitations of human memory. Respondents may also misrepresent answers to portray their actions or the US government in the best light. I sought to address these concerns by speaking with a large number of individuals, cross-referencing responses between officials. I then triangulated their revelations with court documents, media reporting, and other public records as well as with the case studies.

Overall, I spoke with 81 US federal prosecutors and agents and ten foreign officials. These interviews focused on the leadership at the US Department of Justice (USDOJ), who oversee prosecutions around the country and across multiple areas of crime. This perspective means that they could offer the most holistic insights. The case studies employed the method of process-tracing, primarily based on interviews with the key prosecutors and federal agents involved. My goal was to determine the causal factors that led to the use of a unilateral alternative in those prosecutions. This served as a further form of theory testing and theory development.

In Chapter 4, I reported on my findings related to the challenges of securing custody over international cybercriminals. The interview evidence suggested that unilateral alternatives, in the form of lure operations, are indeed applied more often in cybercrime cases as compared to other transnational crimes. Why? I learned that cybercrime indeed suffers from complications related to the facts of the case and political considerations but not any significant legal barriers.

Specifically, law enforcement struggles to identify where cybercriminals are located, let alone prove who was sitting behind the keyboard. Yet, they can deploy a lure operation to smoke him out of hiding. Plus, once the cybercriminal arrives on the lure, it is difficult for him to credibly deny involvement. Additionally, the remote nature of cybercrime enables perpetrators to shelter indefinitely in safe haven countries.

But, why are these countries safe havens? Is it due to legal reasons? I discovered that dual criminality is no longer a major barrier to extradition in cybercrime. This is a result of legal improvements abroad as well as the success of the Budapest Convention. Similarly, the political offense argument typically does not hold water owing to the inherently commercial nature of most cybercrimes. And, jurisdictional conflicts have been resolved through international coordination rather than unilateralism.

So, why can't host countries be relied upon for cooperation? As predicted, many lack the political will to assist. They view cybercrime as a nonviolent offense, oftentimes with a sympathetic perpetrator. Consequently, they can score domestic political points by denying cooperation. After all, the stakes seem lower since these crimes do not engender domestic harms. Other countries take this step further and sponsor cybercrimes. They protect cybercriminals who operate in their territory so that they can later coopt them for state objectives. This has even included interfering in the extradition process when their cybercriminals are arrested while traveling. As a result, pursuing countries frequently have no choice but to lure them to countries from which they can be reliably rendered.

In Chapter 5, I sought to determine what, if any, lessons could be learned from the experience of prosecuting other transnational crimes. I compared cybercrime to terrorism, drug trafficking, fraud and foreign corruption, and export control and sanctions cases. I ultimately concluded that cybercrime is not likely to evolve in the same manner as any of these other offenses and that the need for unilateralism may instead be here to stay.

For example, cybercrime is not likely to progress toward cooperation as occurred in the case of both terrorism and drug trafficking. With those offenses, host countries recognized the substantial domestic harms that the illicit conduct caused and were often eager to assist in handing over the perpetrators. Yet, cybercriminals know not to target their fellow citizens, engendering little, if any, domestic harms. This is precisely why certain states have turned to sponsoring such conduct rather than combatting it.

Likewise, cybercrime prosecutions cannot rely on the perpetrator traveling or engaging in a self-surrender. Those outcomes frequently occur in drug trafficking, fraud and foreign corruption, and export control and sanctions cases. However, the remote nature of cybercrime means that offenders have no business reason to cross borders. They are instead incentivized to remain in the safety of their home country where they can reap

substantial illicit proceeds. Finally, none of the compared offenses suffer from challenges of attribution to the same extent as cybercrime. This means the need for unilateralism to smoke cybercriminals out of hiding and establish their identity will persist.

If unilateralism may indeed be here to stay, states must deploy such methods responsibly so as not to run roughshod over the sovereignty of host countries and human rights of the accused. In Chapter 6, I devised a framework to outline baseline standards for when the use of unilateral lure operations may be prudent in cybercrime cases. This framework could serve as a set of voluntary, non-binding norms to assess the advisability of unilateralism in cybercrime prosecutions. It is informed by the existing legal justifications advanced for unilateral alternatives in war crimes, terrorism, and drug trafficking cases. Yet, it does not seek to settle long-standing debates in international law regarding the permissibility of such tools.

The International Criminal Tribunal for the Former Yugoslavia (ICTY) has found the use of a unilateral alternative is not grounds for setting aside jurisdiction in war crimes cases as long as there are no egregious abuses or torture. Nevertheless, cybercrime is not a universally condemned offense, like war crimes, nor prosecuted by an instrument of the UN Security Council, like the ICTY. This suggests higher standards may be necessary.

Not all terrorist acts are universally condemned nor are these crimes prosecuted by international tribunals. But, unilateral alternatives can still be permissible. The existing legal scholarship suggests that the use of such tools must be necessary and proportionate and the host country must be complicit. However, that last criterion should be relaxed in cybercrime cases to account for the attribution challenge. Otherwise, devastating attacks could continue unabated.

Now looking to a crime that is not necessarily violent, unilateral alternatives can even still be permissible in drug trafficking cases. Similar criteria apply as for terrorism

prosecutions. Yet, the literature suggests that unilateralism is justified in drug trafficking cases, in part, since the crime is committed for private benefit.

Based on these existing legal principles and the findings of this dissertation, I ultimately conclude that lure operations may be most prudent when 1) there are no viable and less intrusive alternatives; 2) there is a significant and imminent threat, 3) the crime is suspected to be motivated by private gain for the accused; 4) law enforcement does not engage in entrapment or coercion; and 5) the accused is guaranteed a fair trial with full due process protections.

7.2 Moving Beyond the US: Generalizability of the Findings

This investigation has primarily focused on US practice with respect to prosecuting cross-border cybercrime. Indeed, nearly 90% of my interviewees were US officials. This raises the question, to what extent do the findings apply to other countries? Or, are the conclusions specific to the US? On the one hand, the US is uniquely positioned on the global stage such that it can withstand backfire from deploying a lure. And it has the investigative experience and resources to deploy such complex methods to secure custody.

On the other hand, the challenges of cybercrime that create the need for unilateralism are not unique to the US. Any country would face the same struggles in definitively locating the perpetrator and proving he was the one sitting behind the keyboard. In fact, these difficulties may be even greater for countries that do not have the same cyber investigative expertise as the US. The need for a lure operation would then be further heightened to smoke the offender out and/or establish his identity.

Likewise, the challenges of state sponsorship cannot be written off as merely due to the adversarial relationship between the US and those host countries either. In the Mabna Institute case, hackers operating under the protection of the Iranian government stole academic data and intellectual property from 176 universities across 21 countries as

well as eleven companies in five countries.[4] Indeed, law enforcement officials from Germany and the Netherlands agreed that they do not receive assistance from state sponsors in bringing to justice cybercriminals who operate there. Those countries rather provide safe haven so that they may later co-opt those offenders for state purposes.

To probe the generalizability of my findings more empirically, I sought to interview officials from eight other countries. As explained in Chapter 6, I learned that the US is not alone in the use of lure operations. Indeed, Belgium, Germany, and Israel have all previously deployed this tool.[5] This suggests lures are not confined to the US due to its global position. In fact, Israel has even used a lure operation in a cyber-related case.

Nevertheless, there are certain considerations that limit the generalizability of this research, at least for now. I learned that other countries are not as proactive in prosecuting cybercriminals located abroad, which mitigates the need for lure operations. For example, New Zealand Crown lawyer Fergus Sinclair explained to me that he "couldn't think of any cases where New Zealand has sought to prosecute a cybercriminal [located] in another country in the last 15 years."[6] Similarly, Brazilian prosecutors shared with me that they tend to focus on prosecuting the members of cybercriminal conspiracies who are located within Brazil.

When other countries have sought to prosecute cybercriminals located overseas, they have generally focused on their nationals who are abroad. For example, a German prosecutor recounted to me, "All the usual cases are Germans having committed the crimes abroad."[7] In such scenarios, cooperation is more likely to succeed. The host country has less of a connection to the perpetrator, so they have less of an incentive to

[4] "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," March 23, 2018.
[5] German Prosecutor, interview; Genesove, "The Highs and Lows of Amos Silver, Telegrass Cannabis Kingpin Nabbed in Ukraine."
[6] Sinclair, interview.
[7] German Prosecutor, interview.

deny assistance. For example, refusing extradition of a foreign national likely would not help local officials score political points.

The other category of cybercrime cases that countries like Brazil and NZ have pursued across borders involve online child exploitation. Again, cooperation is more likely to succeed here since the offenses are universally condemned. Multiple US prosecutors observed that there is "clearly a consensus about child exploitation online and immediacy since in many cases the abuse is ongoing."[8] These crimes "tend to get a rapid, effective response" whereby even countries like China and Russia are willing to cooperate "since there is no economic or security interest."[9] As a result, there would be less of a need to resort to unilateralism.

These differences between how the US and other countries approach cybercrime cases reflect the US's advanced position in prosecuting these offenses. It has greater experience and expertise, so it can focus on the more difficult cases where the evidence and perpetrators are spread around the world. But, that does not mean other countries will always lag behind the US. As they develop experience and expertise, they may adopt a more proactive stance toward prosecuting cybercriminals in other countries. They may then have a reason to deploy lure operations. Thus, the findings of this dissertation may become more generalizable over time. Indeed, one prosecutor remarked that the US is "just a little more developed and mature in our ability to work out these sorts of cases. Other countries are going to get there pretty soon."[10] This prediction is already coming to fruition as Germany has followed in the US's footsteps and issued criminal charges against a state sponsored hacker in Russia.[11]

[8] Prosecutor 18, interview.
[9] Prosecutor 44, interview; Prosecutor 27, interview.
[10] Prosecutor 57, interview.
[11] Cimpanu, "German Authorities Charge Russian Hacker for 2015 Bundestag Hack."

Another factor to consider regarding the generalizability of the findings is that by and large, the US "is a lot more activist and willing to take some swings to get people."[12] Specifically, the "US is very forward thinking on undercover operations in a way the rest of the world is not," and lures tend to arise in that context.[13] In fact, certain countries, like Japan, prohibit the use of undercover operations. Therefore, it would likely be impossible for them to carry out a lure.

Other countries permit undercover operations, but their courts have expressly prohibited the use of lures. This suggests that even as countries develop cybercrime expertise and prosecute more ambitious cases, the findings may not apply to certain jurisdictions where either undercover operations broadly or lures specifically are not permitted under domestic law.

7.3 Implications for International Law and Policy

What do the findings of this dissertation tell us about potential future developments in international law and policy to combat cross-border cybercrime? Over the years, scholars and policymakers have suggested several innovative proposals in international law to overcome the hurdles of bringing cybercriminals to justice. They include drafting a universal cybercrime treaty, extending universal jurisdiction to cybercrime, or forming a cybercrime international tribunal.

However, the results of this study reveal that these solutions will still not address the core difficulties. Indeed, each proposal would still require the prosecuting country or tribunal to lay hands on the cybercriminal but would not create any mechanism to compel the host country to cooperate or overcome the attribution challenge. Nevertheless, important progress in international law could be made in outlining how to prioritize

[12] Prosecutor 28, interview, January 7, 2020.
[13] Prosecutor 52, interview; Prosecutor 44, interview.

competing extradition requests, re-examining the applicability of functional immunity to cybercrime, and clearly defining the acceptable bounds of cyberespionage.

Given the diverging interests between countries, it would be near impossible to reach consensus on a universal cybercrime treaty. On the one hand, pursuing countries wish to prosecute perpetrators through their domestic courts. On the other hand, the most prolific host countries wish to protect cybercriminals. These offenders stimulate the local economy through the influx of illicit proceeds, provide access to foreign intellectual property, and can later be coopted for intelligence goals. This is precisely why there has remained no consensus on the proposed United Nations cybercrime treaty.

Even if such a truly global cybercrime treaty were to be drafted, there is no mechanism under international law to force host countries to sign or bind them by its provisions. In the unlikely event that countries would agree to the treaty, they still could back out or refuse to meaningfully comply at any time. As international relations scholar Robert Keohane admits, "any patterns of legal liability … established in world politics are subject to being overturned by the actions of sovereign states."[14] One prosecutor shared this assessment with respect to cybercrime:

> Honestly, the reason it's so hard to extradite from some countries or impossible is because of very strong entrenched policy on their end. I don't see much we can do to change on our end. I mean let's be honest. Even if we sign a treaty tomorrow with some Eastern European, former Soviet republics … actually doing it versus what we agreed to do would be very different.[15]

Certain scholars have instead suggested adopting universal jurisdiction for cybercrime. This would permit any country to prosecute, regardless of whether they were victimized. Universal jurisdiction has been justified for other offenses based on the heinousness of the conduct. Such a case could be made for cybercrime given the scale of economic losses and invasions of privacy, particularly as offenders steal troves of sensitive

[14] Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy*, 88–89.
[15] Prosecutor 20, interview.

personal information. The case for universal jurisdiction becomes even stronger as cybercrime merges with terrorism and endangers health and safety.[16] The threat from cybercrime is further exacerbated by the relative ease of perpetration, which creates a high likelihood for repeat attacks.[17]

Cybercrime can also be analogized to the first crime subject to universal jurisdiction: piracy. Both occur in a domain beyond the control of any state. Both "threaten international trade and the global economy."[18] This means the international community has an interest in bringing these perpetrators to justice. Therefore, Gable argues that universal jurisdiction may be justified on the basis that the prosecuting country is "acting as an agent for the international community."[19]

Nevertheless, the problems of securing custody over international cybercriminals have not stemmed from an inadequate basis for jurisdiction. Under the principle of territorial jurisdiction, countries can prosecute crimes that occur or result in harm within their territory. Thus, even though cyberspace may exist outside the control of any one country, any victim country can still exert territorial jurisdiction over cybercrimes. This means there is no need to establish a new form of jurisdiction. There is no need to rely on other benevolent countries prosecuting on behalf of the international community.

Equally important, universal jurisdiction still requires the prosecuting country to lay hands on the cybercriminal. Yet, universal jurisdiction does not compel host countries to render these offenders, nor does it resolve the attribution challenge. Consequently, this creates a situation whereby every country can prosecute but none can secure custody.

[16] Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent."
[17] Gable, 113.
[18] Gable, 111.
[19] Gable, 112.

Additionally, scholars have proposed creating an international cybercrime tribunal. This court could be modeled off the International Criminal Court (ICC). It could focus on prosecuting the most significant and heinous cybercrimes and serve as an authoritative source on interpreting cybercrime law. The international nature of the court would also facilitate investigations with evidence, witnesses, and perpetrators in multiple countries.[20]

However, such a cybercrime tribunal would likely suffer from the same shortcomings that have hamstrung the ICC. Primarily, the ICC only has jurisdictions over cases involving states that have accepted its jurisdiction or cases referred by the UN Security Council. Given the role of state sponsorship, the most pernicious host countries of cybercrime would likely never accept such a court's jurisdiction. The UN Security Council route is not a viable alternative either. China and Russia would surely block any referrals against their cybercriminals.

Even if such a court were to proceed, it would face serious issues with enforcement. Similar to the ICC, it would likely operate based on the principle of complementarity. In other words, the court would defer to national courts that wish to prosecute the offense. This runs a significant risk that the host country could announce its intent to prosecute but only pursue a slap-on-the-wrist charge to protect its hackers.

Furthermore, "the ICC lacks police or military forces, let alone its own source of funding, and so it cannot apprehend suspects or enforce its own orders. It is therefore subject to the political whims of a state when requesting that state arrest or surrender a defendant."[21] This again leaves us with the same dilemma. Just as pursuing countries cannot force a host country to hand over one of their citizens, neither will such an international court. Plus, an international cybercrime court would still struggle to prove

[20] Cade, "An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code," 1170–72.
[21] Cade, 1163.

attribution, particularly since it cannot compel recalcitrant host countries to provide evidence or assist in investigations.

One area of international law where improvements can be made relates to competing extradition requests. As described in Chapter 4, state sponsors regularly launch extradition requests when one of their cybercriminals is arrested in a third country. The state sponsor may win since there is no set criteria for the arresting country to prioritize the requests. Such competing claims also delay the extradition process. This often results in the defendant being released on bail, allowing him to flee to safety in his home country.

Establishing international agreement in this area could address both concerns. Clear criteria would ensure that those countries with a legitimate interest in justice prevail. Clear criteria would also expedite the process, eliminating the need to release these offenders on bail and foiling their chances of escape. For example, requests could be prioritized by the degree of harm alleged by each country. As prosecutors explained, the competing requests from countries such as Russia are for minor charges.[22]

While state sponsors could still game this system by alleging higher losses, the optics would be far from optimal. It would require them to admit that large-scale cybercrimes emanate from their territory. It would also shine a greater spotlight on them if they do not meaningfully prosecute the case. Additionally, if extradition requests are prioritized by the alleged harm, there is a concern that state sponsors could launch retaliatory extradition requests against citizens of the pursuing country who are located abroad. They could allege significant losses to ensure their request prevails. Therefore, competing extradition requests should first be evaluated to ensure there is a legitimate case and the prosecution is not politically motivated. Then, the alleged losses can be compared.

[22] Prosecutor 29, interview, August 13, 2019.

Even though these changes would facilitate the extradition process, host countries could still find other ways to interfere. They could follow the example of China and Iran by threatening retaliation against the arresting country unless that country denies extradition. Establishing criteria to prioritize extradition requests would not address this concern. It would also not resolve most cybercrime cases where the perpetrator never leaves the safety of his home country. Nor would it enable cases to proceed when the pursuing country struggles to establish attribution.

Therefore, even the most innovative policy proposals for reforming international law cannot overcome the core challenges to securing custody over cybercriminals revealed by this dissertation. If countries wish to lay their hands on cybercriminals, then unilateralism may remain a pragmatic inevitability. Thus far, this dissertation has explored the potential advantages and disadvantages of unilateral alternatives in specific cases. These benefits include ending ongoing attacks, allowing law enforcement to penetrate cybercriminal networks, and vindicating victims.

Yet, I learned that lure operations may also have broader policy implications by serving as a general deterrent to cybercrime. A federal agent explained to me that as law enforcement infiltrates cybercriminal organizations through lures, they can erode trust, which "really does slow down their ability to work."[23] The agent elaborated, "The more successful these lure operations become, the more guarded and conservative some of these folks will be, not knowing who you're talking to."[24] As a result, the scope of their conspiracies and the damage that they can cause may be limited.

However, such infiltration may not be possible with every lure. So, can these operations still serve as a general deterrent? Prosecutors explained to me that luring,

[23] Federal Agent 11, interview, August 22, 2019.
[24] Federal Agent 11, interview, February 18, 2020.

arresting, and prosecuting key perpetrators can send a message to other cybercriminals, altering their decisional calculus. According to former Deputy Assistant Attorney General of USDOJ's Criminal Division Jason Weinstein, perpetrators "view cybercrime as very high reward and low risk because they think they are anonymous or can't be caught or they reside in safe haven countries. You have to show people who thought they were out of your reach that they are within your reach."[25]

The costs of being arrested and incarcerated in a foreign prison are significant, especially if the prosecution also results in seizing the offender's assets. Cybercriminals tend to be well-informed regarding law enforcement activity. So, knowledge of successful prosecutions may cause them to second-guess pursuing this illicit conduct. Another prosecutor agreed, "If you make it clear that you take a swing at them and traditional methods of obfuscation will not work, then you can post hoc prevent future crimes."[26]

Nevertheless, the deterrent value of criminal prosecutions on governments that act as state sponsors may be limited. As former AAG-NSD David Kris acknowledged, "President Xi Jinping or Vladimir Putin may not care that much if we prosecute an individual foot soldier."[27] However, many individuals committing state sponsored cybercrimes are ordinary cybercriminals moonlighting for the state. If the threat of prosecution discourages these individuals from becoming cybercriminals, it can shrink the talent pool available for state sponsors to coopt. Moreover, it may discourage state actors from committing cybercrimes on the side for their own profit.

Despite these advantages of lures touted by US law enforcement officials, policymakers must not lose sight of the potential costs of such operations. As previously outlined, some members of the international community may believe they breach

[25] Weinstein, interview, January 10, 2020.
[26] Prosecutor 28, interview, January 7, 2020.
[27] Kris, interview.

international law by violating the sovereignty of the host country and due process rights of the accused. If they are regularly deployed, lures may then have a broader impact in undermining respect for international law. They may also cause countries to question to validity of the extradition system, which plays a central role in countless cross-border cases, and to hesitate joining new mutual legal assistance agreements. Furthermore, such operations may undermine international stability if they are recklessly deployed and host countries begin engaging in retaliation.

Hence, any future lure operations should be deployed in line with the framework expounded in Chapter 6. This will minimize the likelihood of causing the above negative consequences and generating backlash from elements of the international community. However, the framework raises its own questions for the future of international law and policy. Specifically, the functional immunity that state actors enjoy for cybercrimes committed in their official capacity will permit significant injustices to linger. As Rowe notes, "state backing provides a level of organization and funding to hackers which a typical individual hacker is unlikely to possess … This creates a dynamic where individual private companies are trying to defend against cyber intrusions by a nation."[28]

These concerns are epitomized by the February 2021 US indictment of three computer programmers for the North Korean Reconnaissance General Bureau. Among other offenses, these intelligence officers stand accused of hacking banks around the world to steal over $1.2 billion, launching the destructive WannaCry 2.0 ransomware to extort money from victim companies, and pilfering over $110 million in cryptocurrency. These acts are all modern-day forms of robbery and clearly criminal conduct. Yet, as USDOJ alleges, the conspiracy served to "further the strategic and financial interests of the DPRK

[28] Rowe, "Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire," 65.

government and its leader, Kim Jong Un."[29] Therefore, such conduct may be covered by functional immunity, and a lure operation would not be prudent under my framework.

In the past, such quandaries of functional immunity were rarer since foreign officials typically could not commit crimes without physically being present in the victim country. Cybercrime completely changes that dynamic. State actors can now easily project themselves into victim countries. They can commit common crimes yet remain protected from criminal prosecution abroad since they did so in their official capacity. This injustice suggests that international law and policy must evolve to address this new and unprecedented threat. However, a blanket territorial exemption from immunity, like that suggested by US officials in Chapter 6, risks creating a global free-for-all. Even government officials engaging in legitimate forms of cyberespionage could then be lured and prosecuted by the countries they hacked.

Instead, international lawyers and policymakers should focus on developing rules regarding the acceptable bounds of cyberespionage when committed on behalf of a state. Acts perpetrated for private gain, regardless of whether they meet the definition of cyberespionage, would qualify for lures. Likewise, nation-state cyber activity that crosses the acceptable lines of cyberespionage would be eligible for a lure operation. However, legitimate national security activity would continue to be covered under functional immunity and thus exempt from lures and criminal prosecutions. As Akande and Shah note, new rules of international law may supersede older provisions of functional immunity.[30] Since cyberespionage exists on a spectrum, the task for international policymakers is now to determine where that line between acceptable and criminal conduct by states falls.

---

[29] "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe."
[30] Akande and Shah, "Immunities of State Officials, International Crimes, and Foreign Domestic Courts," 840.

The *Tallinn Manual 2.0*'s definition of cyberespionage can provide a starting point. Cyberespionage "refers to any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information. Cyber espionage involves, but is not limited to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information."[31] Adopting this definition would exclude the North Korean bank heists.

However, the definition does not distinguish between cyberespionage for national security and commercial purposes. The former is a widely accepted practice. In contrast, certain countries, such as the US, stridently object to the latter as beyond the pale. While resolving this complex debate on economic espionage is beyond the scope of this dissertation, it should be an important consideration for international lawyers and policymakers in determining the acceptable bounds of cyberespionage.

7.4 Directions for Future Research

Additional research may be able to shed light on several open areas related to the challenges of bringing transnational criminals to justice and the methods used to secure custody that laid beyond the scope of this dissertation. For example, a future study could engage in a more comprehensive review of experiences and practices in prosecuting cybercrime beyond the US. I sought to accomplish this by speaking with officials from other countries. However, those ten interviews only scratched the surface. Such a future analysis could follow a similar methodology, interviewing the top cybercrime prosecutors and investigators in countries across all continents. Those interviews could seek to identify how the challenges of prosecuting cross-border cybercrime, methods used to secure custody, and legality of alternatives to extradition differ between countries. Those

[31] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 168.

conversations would provide further insights regarding the generalizability of my findings and framework.

Likewise, another study could take a closer look at the other types of transnational crime that I examined. Through my research, I determined that each of those offenses, namely terrorism, drug trafficking, fraud and foreign corruption, and export control and sanctions violations, face less of a need for unilateralism than cybercrime. Nevertheless, unilateralism is still deployed at times to combat those crimes. Therefore, future research could employ the case study method I utilized to dig deeper into those anomalous cases employing unilateral alternatives.

The goal would be to determine why the US resorted to such mechanisms. This would help determine whether my theory that the need for unilateralism stems from challenges related to the facts of the case (i.e., the attribution challenge) and political complications (i.e., lack of political will or state sponsorship) applies beyond cybercrime.

Such findings could help determine whether the same framework I propose for the use of lure operations in cybercrime would be appropriate for those other offenses. Indeed, there are not yet any such frameworks, to my knowledge, for fraud and foreign corruption or export control and sanctions cases. Plus, the existing frameworks for terrorism and drug trafficking prosecutions cited in Chapter 6 were mainly devised in the 1980s, 1990s, and early 2000s. So, they may need to be updated as these crimes and the prospects for securing custody have evolved over time.

Finally, a further study could examine the effectiveness of lure operations in cybercrime cases. This could involve interviews with some of the same prosecutors and agents who participated in my research. However, the interview questions would focus on the usefulness of lures and the factors that made certain operations more successful than others. Such an investigation could also interview cybercriminals, particularly those

targeted for lure operations, to determine why they fell for the inducement or not. Moreover, interviews with cybercriminals can probe the extent to which lures have any impact as a general deterrent. These findings may suggest refinements to my framework to advise countries when the use of a lure may be most prudent. The results could also help law enforcement officials shape such operations to maximize the likelihood of success.

Overall, this dissertation has sought to help us understand why unilateralism may prevail in cybercrime cases. In doing so, it has uncovered key obstacles to laying hands on cybercriminals located abroad. The findings have also suggested that cybercrime is not likely follow the same evolution toward cooperation as other transnational crimes. Nevertheless, the conversation must not end here. Rather, by further exploring the issues raised by this study and actively engaging with government officials, future academic research can play an important role in helping formulate legal, ethical, and effective policy responses to the challenges of cybercrime.

BIBLIOGRAPHY

U.S. Department of Justice. "9-15.000 - International Extradition and Related Matters," June 2018. https://www.justice.gov/jm/jm-9-15000-international-extradition-and-related-matters.

Abramovsky, Abraham, and Steven J. Eagle. "U.S. Policy in Apprehending Alleged Offenders Abroad: Extradition, Abduction, or Irregular Rendition." *Oregon Law Review* 57, no. 1 (1977): 51–93.

Akande, Dapo, and Sangeeta Shah. "Immunities of State Officials, International Crimes, and Foreign Domestic Courts." *European Journal of International Law* 21, no. 4 (2010): 815–52. https://doi.org/10.1093/ejil/chq080.

Albright, David, Paul Brannan, and Andrea Scheel Stricker. "Case Study - Middleman Majid Kakavand Arrested for Malaysia-Based Iranian Illicit Procurement Scheme." Institute for Science and International Security, February 16, 2010. https://isis-online.org/isis-reports/detail/middleman-arrested-for-directing-malaysia-based-iranian-illicit-procurement.

U.S. Department of Justice. "Alleged Hacker Indicted in New Jersey for Data Breach Conspiracy Targeting Government Agency Networks," October 28, 2013. https://www.justice.gov/usao-nj/pr/alleged-hacker-indicted-new-jersey-data-breach-conspiracy-targeting-government-agency.

Anderson, J. "Piracy and World History: An Economic Perspective on Maritime Predation." *Journal of World History* 6, no. 2 (1995): 175.

Antony, Robert J. "Turbulent Waters: Sea Raiding in Early Modern South East Asia." *The Mariner's Mirror* 99, no. 1 (2013): 23–38. https://doi.org/10.1080/00253359.2013.766996.

Arnold, Aaron, and Daniel Salisbury. "The Long Arm: How U.S. Law Enforcement Expanded Its Extraterritorial Reach to Counter WMD Proliferation Networks." Cambridge, MA: Belfer Center for Science and International Affairs, February 2019. https://www.belfercenter.org/sites/default/files/2019-02/TheLongArm.pdf.

Avergun, Jodi. Interview by Christopher D'Urso. In-Person, August 21, 2019.

———. Interview by Christopher D'Urso. Telephone, September 25, 2020.

Bajak, Frank. "FBI Warns Ransomware Assault Threatens US Healthcare System." Associated Press News, October 29, 2020. https://apnews.com/article/fbi-warns-ransomware-healthcare-system-548634f03e71a830811d291401651610.

Bassiouni, M. Cherif. "Human Rights in the Context of Criminal Justice: Identifying International Procedural Protections and Equivalent Protections in National Constitutions." *Duke Journal of Comparative & International Law* 3, no. 2 (1993): 235–97.

———. *International Extradition: United States Law and Practice*. Sixth. Oxford Scholarly Authorities on International Law. Oxford: Oxford University Press, 2014.

———. "Unlawful Seizures and Irregular Rendition Devices as Alternatives to Extradition." *Vanderbilt Journal of Transnational Law* 7, no. 1 (Winter 1973): 25–70.

Beckmann, Matthew N., and Richard L. Hall. "Elite Interviewing in Washington, DC." In *Interview Research in Political Science*, edited by Layna Mosley, 196–208. Ithaca, NY: Cornell University Press, 2013.

Benton, Lauren A., and Lisa Ford. *Rage for Order: The British Empire and the Origins of International Law, 1800-1850*. Cambridge, Massachusetts: Harvard University Press, 2018.

Bernik, Igor, and Jean-Charles Pomerol. *Cybercrime and Cyberwarfare*. Focus Series in Information Systems, Web and Pervasive Computing. London: ISTE Ltd/John Wiley and Sons Inc, 2014.

Blatter, Joachim, and Markus Haverland. *Designing Case Studies: Explanatory Approaches in Small-N Research*. Research Methods Series. New York: Palgrave Macmillan, 2014.

Boed, Roman. "State of Necessity as a Justification for Internationally Wrongful Conduct." *Yale Human Rights and Development Law Journal* 3, no. 1 (2000): 1–43.

Boister, Neil. *An Introduction to Transnational Criminal Law*. Oxford Scholarly Authorities on International Law. Oxford: Oxford University Press, 2012.

———. "Responding to Transnational Crime: The Distinguishing Features of Transnational Criminal Law." In *Legal Responses to Transnational and International Crimes: Towards an Integrative Approach*, edited by Harmen van der Wilt and Christophe Paulussen, 27–49. Elgaronline. Cheltenham, UK: Edward Elgar Publishing Limited, 2017.

———. "Transnational Criminal Law?" *European Journal of International Law* 14, no. 5 (2003): 953–76. https://doi.org/10.1093/ejil/14.5.953.

Brady, Scott W. "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations." Washington, DC, October 4, 2018. https://www.justice.gov/opa/video/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

Bratt, Jay. Interview by Christopher D'Urso. In-Person, January 7, 2020.

Brenner, Susan W. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Ebook Central. Boston: Northeastern University Press, 2012.

———. "Cybercrime Jurisdiction." *Crime, Law and Social Change* 46, no. 4 (2006): 189–206. https://doi.org/10.1007/s10611-007-9063-7.

———. "Distributed Security: A New Model of Law Enforcement." *Journal of Internet Law* 8, no. 5 (2004): 1.

———. "Is There Such a Thing as 'Virtual Crime'?" *California Criminal Law Review* 4 (n.d.).

Breuer, Lanny. Interview by Christopher D'Urso. In-Person, September 4, 2019.

Brown, Cameron. "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice." *International Journal of Cyber Criminology* 9, no. 1 (2015): 55–119. https://doi.org/10.5281/zenodo.22387.

Cade, Nicholas W. "An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code." *Brooklyn Journal of International Law* 37, no. 3 (2012): 1139–75.

Calica, Andrew J. "Self-Help Is the Best Kind: The Efficient Breach Justification for Forcible Abduction of Terrorists." *Cornell International Law Journal* 37, no. 2 (2004): 389–430.

Government of Canada. "Canada Identifies Malicious Cyber-Activity by Russia," October 4, 2018. https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html.

Carlin, John. "Cyber Space with John Carlin (Ft. John Demers)." Cyber Space with John Carlin, n.d. Accessed June 28, 2020.

Carlin, John P. *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. New York: Public Affairs, 2018.

Cha, Ariana Eunjung. “A Tempting Offer for Russian Pair.” The Washington Post, May 19, 2003. https://www.washingtonpost.com/archive/politics/2003/05/19/a-tempting-offer-for-russian-pair/2c6a5407-8378-4939-8491-038efab2c5fb/.

Council of Europe. “Chart of Signatures and Ratifications of Treaty 185,” January 28, 2021. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=DOzYeqZn.

Chernukhin, Ernest. “Countering the Use of Information and Communication Technologies for Criminal Purposes.” Presented at the Council of Europe Octopus Conference on Cooperation Against Cybercrime, Strasbourg, France, November 20, 2019.

Ministry of Foreign Affairs of the People’s Republic of China. “China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel,” May 20, 2014. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1157520.shtml.

U.S. Department of Justice. “Chinese Citizen Sentenced to 12 Years in Prison for Cyber-Theft and Piracy of Over $100 Million in Sensitive Software and Proprietary Data,” June 11, 2013. https://www.justice.gov/usao-de/pr/chinese-citizen-sentenced-12-years-prison-cyber-theft-and-piracy-over-100-million.

Law360. “Chinese National Arrested in Carbon Fiber Smuggling Sting,” April 14, 2016. https://www.law360.com/newyork/articles/784853/chinese-national-arrested-in-carbon-fiber-smuggling-sting.

U.S. Department of Justice. “Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors’ Systems to Steal Sensitive Military Information,” March 23, 2016. https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive.

U.S. Department of Justice. “Chinese National Who Conspired to Hack into U.S. Defense Contractors’ Systems Sentenced to 46 Months in Federal Prison,” July 13, 2016. https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months.

Cimpanu, Catalin. “Five Other Countries Formally Accuse China of APT10 Hacking Spree.” ZDNet, December 21, 2018. https://www.zdnet.com/article/five-other-countries-formally-accuse-china-of-apt10-hacking-spree/.

———. “German Authorities Charge Russian Hacker for 2015 Bundestag Hack.” ZDNet, May 5, 2020. https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/.

Clough, Jonathan. “A World of Difference: The Budapest Convention and the Challenges of Harmonisation.” *Monash University Law Review* 40, no. 3 (2014): 698–736.

———. *Principles of Cybercrime*. Second. Cambridge: Cambridge University Press, 2015.

Condliffe, Jamie. “A History of Yahoo Hacks.” MIT Technology Review, December 15, 2016. https://www.technologyreview.com/2016/12/15/106901/a-history-of-yahoo-hacks/.

Creswell, John W, and Vicki L Plano Clark. *Designing and Conducting Mixed Methods Research*. 2nd ed. Los Angeles, Calif.: SAGE, 2011.

United Nations Office on Drugs and Crime. “Cyberwarfare Module,” June 2019. https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html.

Manhattan District Attorney’s Office. “DA Vance: Ringleader of International Cyber Fraud Ring Sentenced to 4-to-12 Years in State Prison for StubHub E-Ticket

Scheme," July 6, 2016. https://www.manhattanda.org/da-vance-ringleader-international-cyber-fraud-ring-sentenced-4-12-years-state-prison-s/.
D'Ambrosio, Michael. Interview by Christopher D'Urso. In-Person, August 22, 2019.
Dandurand, Yvon, and Vivienne Chin. "Implementation of Transnational Criminal Law: Issues and Challenges." In *Routledge Handbook of Transnational Criminal Law*, edited by Neil Boister and Robert J Currie, 436–52. Handbook of Transnational Criminal Law. Abingdon, Oxon: Routledge, 2015.
Denton, Dave. Interview by Christopher D'Urso. In-Person, September 6, 2019.
DeYoung, Karen, Adam Goldman, and Julie Tate. "U.S. Captured Benghazi Suspect in Secret Raid." The Washington Post, June 17, 2014. https://www.washingtonpost.com/world/national-security/us-captured-benghazi-suspect-in-secret-raid/2014/06/17/7ef8746e-f5cf-11e3-a3a5-42be35962a52_story.html.
Doyle, David. "McKinnon and Ahsan: A Tale of Two Extraditions." Channel 4 News, October 16, 2012. https://www.channel4.com/news/mckinnon-and-ahsan-a-tale-of-two-extraditions.
DuBose, Michael. Interview by Christopher D'Urso. Telephone, January 10, 2020.
Dwyer, Johnny. "The U.S. Quietly Released Afghanistan's 'Biggest Drug Kingpin' From Prison. Did He Cut a Deal?" The Intercept, May 1, 2018. https://theintercept.com/2018/05/01/haji-juma-khan-afghanistan-drug-trafficking-cia-dea/.
Eddy, Melissa, and Nicole Perlroth. "Cyber Attack Suspected in German Woman's Death." The New York Times, September 18, 2020. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.
Efrat, Asif. "Cross-National Interviewing at International Conferences: How to Make the Most of a Unique Research Opportunity." *International Studies Perspectives* 16, no. 3 (2015): 302–11. https://doi.org/10.1111/insp.12065.
Eoyang, Mieke, Allison Peters, Ishan Mehta, and Brandon Gaskew. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, October 29, 2018. https://thirdway.imgix.net/pdfs/override/To_Catch_A_Hacker_Report.pdf.
Erlanger, Steven, and Nadim Audi. "France Won't Extradite Iranian Sought by U.S." The New York Times, May 5, 2010. https://www.nytimes.com/2010/05/06/world/europe/06france.html.
Evans, Alona. "Acquisition of Custody over the International Fugitive Offender - Alternatives to Extradition: A Survey of United States Practice." *British Yearbook of International Law* 40 (1964): 77.
The White House. "Fact Sheet: President Xi Jinping's State Visit to the United States," September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
Farivar, Cyrus. "After Silk Road Takedowns, Dark Web Drug Sites Still Thriving." Ars Technica, December 19, 2014. https://arstechnica.com/information-technology/2014/12/after-two-silk-road-takedowns-dark-web-drug-sites-still-thriving/.
Federal Agent 5. Interview by Christopher D'Urso. Telephone, January 17, 2020.
Federal Agent 7. Interview by Christopher D'Urso. In-Person, September 6, 2019.
———. Interview by Christopher D'Urso. Telephone, March 17, 2021.
Federal Agent 9. Interview by Christopher D'Urso. In-Person, August 21, 2019.
Federal Agent 11. Interview by Christopher D'Urso. In-Person, August 22, 2019.

———. Interview by Christopher D'Urso. Telephone, February 18, 2020.
———. Interview by Christopher D'Urso. Telephone, September 16, 2020.
Federal Agent 12. Interview by Christopher D'Urso. Telephone, February 12, 2020.
———. Interview by Christopher D'Urso. Telephone, September 15, 2020.
Feinrider, Martin. "Extraterritorial Abductions: A Newly Developing International Standard." *Akron Law Review* 14, no. 1 (Summer 1980): 27–48.
Fernandez, Manny, and Mitchell Ferman. "El Chapo Highlighted Mexican Corruption, but Drug Money Also Lubricates U.S. Border." The New York Times, February 18, 2019. https://www.nytimes.com/2019/02/18/us/drugs-crossing-border.html.
Feuer, Alan. "El Chapo Trial Shows That Mexico's Corruption Is Even Worse than You Think." The New York Times, December 28, 2018. https://www.nytimes.com/2018/12/28/nyregion/el-chapo-trial-mexico-corruption.html.
Findlay, D. Cameron. "Abducting Terrorists Overseas for Trial in the United States: Issues of International and Domestic Law." *Texas International Law Journal* 23, no. 1 (Winter 1988): 1–54.
International Criminal Tribunal for the Former Yugoslavia. "First Witnesses to Give Evidence in Open Court in the Nikolic Case," October 4, 1995. https://www.icty.org/en/sid/7226.
Fletcher, Andrew K. "Pirates and Smugglers: An Analysis of the Use of Abductions to Bring Drug Traffickers to Trial." *Virginia Journal of International Law* 32, no. 1 (1992 1991): 233–64.
U.S. Department of Justice. "Foreign Corrupt Practices Act," February 3, 2017. https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.
Bivonas Law. "Forum Bar - Finally in Force?," September 27, 2018. https://www.bivonaslaw.com/forum-bar-finally-in-force/.
Digital Shadows. "Forums Are Forever – Part 1: Cybercrime Never Dies," December 4, 2019. https://www.digitalshadows.com/blog-and-research/forums-are-forever-part-1-cybercrime-never-dies/.
Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent." *Vanderbilt Journal of Transnational Law* 43, no. 1 (2010): 57.
Genesove, Ziv. "The Highs and Lows of Amos Silver, Telegrass Cannabis Kingpin Nabbed in Ukraine." The Times of Israel, March 23, 2019. https://www.timesofisrael.com/the-highs-and-lows-of-amos-silver-telegrass-cannabis-kingpin-nabbed-in-ukraine/.
George, Alexander L., and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005.
German Prosecutor. Interview by Christopher D'Urso. Video Call, January 11, 2021.
Gerring, John. *Case Study Research: Principles and Practices*. Cambridge: Cambridge University Press, 2007.
Goldman, Adam, and Eric Schmitt. "Benghazi Attacks Suspect Is Captured in Libya by U.S. Commandos." The New York Times, October 30, 2017. https://www.nytimes.com/2017/10/30/world/africa/benghazi-attacks-second-suspect-captured.html.
Goldsmith, Jack. "Cybersecurity Treaties: A Skeptical View." Palo Alto, CA: Hoover Institution, February 2011. https://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

Goodman, Marc D, and Susan W Brenner. “The Emerging Consensus on Criminal Conduct in Cyberspace.” *International Journal of Law and Information Technology* 10, no. 2 (2002): 139–223. https://doi.org/10.1093/ijlit/10.2.139.
Gough, Barry M. *Pax Britannica: Ruling the Waves and Keeping the Peace before Armageddon*. Britain and the World. Basingstoke: Palgrave Macmillan, 2014.
U.S. Department of Justice. “GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation,” May 16, 2019. https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled.
Grabosky, Peter. “The Global Dimension of Cybercrime.” *Global Crime* 6, no. 1 (2004): 146–57. https://doi.org/10.1080/1744057042000297034.
Grabosky, Peter N. “Virtual Criminality: Old Wine in New Bottles?” *Social & Legal Studies* 10, no. 2 (2001): 243–49. https://doi.org/10.1177/a017405.
U.S. Department of Justice. “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election,” July 13, 2018. https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.
U.S. Department of Justice. “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election,” July 13, 2018. https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.
“Guidelines on International Protection No. 5: Application of the Exclusion Clauses: Article 1F of the 1951 Convention Relating to the Status of Refugees.” UN High Commissioner for Refugees, September 4, 2003. https://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3f5857684.
Gurulé, Jimmy. “Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad.” *Hastings International and Comparative Law Review* 17, no. 3 (Spring 1994): 457–96.
U.S. Department of Justice. “Haji Bagcho Sentenced to Life in Prison on Drug Trafficking and Narco-Terrorism Charges,” June 12, 2012. https://www.justice.gov/opa/pr/haji-bagcho-sentenced-life-prison-drug-trafficking-and-narco-terrorism-charges.
Hakmeh, Joyce, and Allison Peters. “A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet.” Council on Foreign Relations, January 13, 2020. https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.
Hall, David Locke. *CRACK99: The Takedown of a $100 Million Chinese Software Pirate*. New York: W.W. Norton & Company, 2015.
———. Interview by Christopher D’Urso. In-Person, August 27, 2019.
Ham, Marc van der. Interview by Christopher D’Urso. Video Call, January 29, 2021.
Hayes, Ben, Julien Jeandesboz, Francesco Ragazzi, Stephanie Simon, and Valsamis Mitsilegas. “The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-Up?” Luxembourg: European Parliament Direcorate-General for Internal Policies, 2015. https://doi.org/10.2861/996881.
Hendry, James. “Determining Whether a Case Has Sufficient Gravity to Be Admissible at the International Criminal Court (ICC).” *PKI Global Justice Journal* 4, no. 7 (2020).
Hess, Amy. Interview by Christopher D’Urso. In-Person, August 21, 2019.
Horsley, Evans F. “State-Sponsored Ransomware Through the Lens of Maritime Piracy.” *Georgia Journal of International and Comparative Law* 47, no. 3 (2019): 669–81.

Hotten, Russell. “Volkswagen: The Scandal Explained.” BBC News, December 10, 2015. https://www.bbc.com/news/business-34324772.
Hsu, Spencer S. “Benghazi Terror Suspect Is in U.S. Court. So Is an FBI Agent Who Captured Him.” The Washington Post, May 10, 2017. https://www.washingtonpost.com/local/public-safety/benghazi-terror-suspects-capture-interrogation-scrutinized-in-federal-court/2017/05/09/304689d8-34dc-11e7-b412-62beef8121f7_story.html.
Hui, Kl, Sh Kim, and Qh Wang. “Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks.” *MIS Q.* 41, no. 2 (2017): 497–523. https://doi.org/10.25300/MISQ/2017/41.2.08.
U.S. Department of Justice. “Hungarian Citizen Sentenced in Maryland to 30 Months in Prison for Hacking into Marriott Computers to Extort Employment from the Company,” February 3, 2012. https://www.justice.gov/opa/pr/hungarian-citizen-sentenced-maryland-30-months-prison-hacking-marriott-computers-extort.
“Identified Foreign Captures.” Human Rights First. Accessed June 22, 2020. https://www.humanrightsfirst.org/sites/default/files/Identified-Foreign-Captures.pdf.
United Nations Treaty Collection. “International Covenant on Civil and Political Rights,” March 29, 1967. https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf.
Israeli Law Enforcement Official. Interview by Christopher D’Urso. Telephone, February 4, 2020.
Joutsen, Matti. “International Instruments on Cooperation in Responding to Transnational Crime.” In *Handbook of Transnational Crime and Justice*, edited by Philip L. Reichel and Jay S. Albanese, Second., 303–22. Thousand Oaks: SAGE Publications, Inc, 2013.
Kallenbach, Charles. “Plomo O Plata: Irregular Rendition as a Means of Gaining Jurisdiction over Colombian Drug Kingpins.” *New York University Journal of International Law and Politics* 23, no. 1 (1991 1990): 169–216.
Keith, Hugo. Interview by Christopher D’Urso. Video Call, January 5, 2021.
Keitner, Chimène. “Trump, Huawei, and the Politics of Extradition: Making Sense of the Meng Case.” Foreign Affairs, January 25, 2019. https://www.foreignaffairs.com/articles/canada/2019-01-25/trump-huawei-and-politics-extradition.
Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton Paperbacks. Princeton, N.J.: Princeton University Press, 1984.
Kerkhofs, Jan. Interview by Christopher D’Urso. Telephone, February 10, 2020.
Kovac, Mary Alice. “Apprehension of War Crimes Indictees: Should the United Nations’ Courts Outsource Private Actors to Catch Them.” *Catholic University Law Review* 51, no. 2 (2002 2001): 619–54.
Krebs, Brian. “Alleged Romanian Subway Hackers Were Lured to US.” Krebs on Security, June 6, 2012. https://krebsonsecurity.com/2012/06/alleged-romanian-subway-hackers-were-lured-to-u-s/.
Kris, David. Interview by Christopher D’Urso. Telephone, January 10, 2020.
Landay, Jonathan. “China Coerces Hundreds of Chinese-Born Critics in U.S. to Return Home, FBI Chief Says.” Reuters, July 7, 2020. https://www.reuters.com/article/us-usa-china-wray/china-coerces-hundreds-of-chinese-born-critics-in-u-s-to-return-home-fbi-chief-says-idUSKBN24825V.
Law Enforcement Official 1. Interview by Christopher D’Urso. In-Person, August 20, 2019.

Law Enforcement Official 2. Interview by Christopher D'Urso. In-Person, August 20, 2019.
Law Enforcement Official 3. Interview by Christopher D'Urso. In-Person, September 25, 2019.
———. Interview by Christopher D'Urso. Email, June 7, 2021.
Law, Jonathan, and Elizabeth A. Martin. "Political Offence." In *A Dictionary of Law*. Oxford: Oxford University Press, 2014.
Leech, Beth L., Frank R. Baumgartner, Jeffrey M. Berry, Marie Hojnacki, and David C. Kimball. "Lessons from the 'Lobbying and Policy Change' Project." In *Interview Research in Political Science*, edited by Layna Mosley, 209–24. Ithaca, NY: Cornell University Press, 2013.
Levin, Dan. "Couple Held in China Are Free, but 'Even Now We Live Under a Cloud.'" The New York Times, January 1, 2017. https://www.nytimes.com/2017/01/01/world/canada/canadian-couple-china-detention.html.
U.S. Department of Justice. "London, England Hacker Indicted Under Computer Fraud and Abuse Act for Accessing Military Computers," November 12, 2002. https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/mckinnonIndict.htm.
Lusthaus, Jonathan. *Industry of Anonymity: Inside the Business of Cybercrime*. Cambridge, Massachusetts: Harvard University Press, 2018.
Government Communications Security Bureau. "Malicious Cyber Activity Attributed to Russia," October 4, 2018. https://www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/.
Martin, Cathie Jo. "Crafting Interviews to Capture Cause and Effect." In *Interview Research in Political Science*, edited by Layna Mosley, 109–24. Ithaca, NY: Cornell University Press, 2013.
Maurer, Tim. "Why the Russian Government Turns a Blind Eye to Cybercriminals." Slate, February 2, 2018. https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html.
Maurushat, Alana. "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?" *University of New South Wales Law Journal* 33, no. 2 (2010): 431–73.
May, Theresa. "Theresa May Statement on Gary McKinnon Extradition." GOV.UK, October 16, 2012. https://www.gov.uk/government/news/theresa-may-statement-on-gary-mckinnon-extradition.
McAlister, Edmund S. "The Hydraulic Pressure of Vengeance: United States v. Alvarez-Machain and the Case for a Justifiable Abduction." *DePaul Law Review* 43, no. 2 (1994 1993): 449–522.
McCarthy, Peter S. "United States v. Verdugo-Urquidez: Extending the Ker-Frisbie Doctrine to Meet the Modern Challenges to Posed by the International Drug Trade." *New England Law Review* 27, no. 4 (1993 1992): 1067–1100.
McCord, Mary. Interview by Christopher D'Urso. In-Person, August 14, 2019.
———. Interview by Christopher D'Urso. Zoom, August 6, 2020.
McDermott, Helen. "Seeking a Stay of Proceedings for Irregular Apprehension before International Courts." *Journal of International Criminal Justice* 14, no. 1 (2016): 145–69. https://doi.org/10.1093/jicj/mqv080.

———. “The Structure of International Cooperation in the Transfer of Suspects. Extradite or Abduct?” *International Criminal Law Review* 15, no. 2 (2015): 254–97. https://doi.org/10.1163/15718123-01502002.
McFadden, Trevor. Interview by Christopher D’Urso. In-Person, August 7, 2019.
McGuinness, Damien. “How a Cyber Attack Transformed Estonia.” BBC News, April 27, 2017. https://www.bbc.com/news/39655415.
Morgan, Steve. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” Cybercrime Magazine, November 13, 2020. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
———. “Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021.” Cybercrime Magazine, October 21, 2019. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/.
Mosley, Layna. “‘Just Talk to People’? Interviews in Contemporary Political Science.” In *Interview Research in Political Science*, edited by Layna Mosley, 1–30. Ithaca, NY: Cornell University Press, 2013.
Nadelmann, Ethan. “The Evolution of United States Involvement in the International Rendition of Fugitive Criminals.” *New York University Journal of International Law and Politics* 25, no. 4 (1993): 813–85.
New York County District Attorney’s Office. “News Release - August 16, 2007,” August 16, 2007. http://manhattanda.org/whatsnew/press/2007-08-16.shtml.
U.S. Department of Justice. “Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps,” March 23, 2018. https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.
U.S. Department of Justice. “Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps,” March 23, 2018. https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic.
The Local. “Norway Refuses to Send Russian ‘Hacker’ to US,” April 27, 2015. https://www.thelocal.no/20150427/norway-refuses-to-extradite-russian-hacker-to-us.
Association for Progressive Communications. “Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online,” August 14, 2020. https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.
The United States Department of Justice. “Overseas Work,” February 19, 2019. https://www.justice.gov/criminal-ccips/overseas-work.
Painter, Christopher. Interview by Christopher D’Urso. In-Person, August 7, 2019.
Pastore, James. Interview by Christopher D’Urso. Telephone, September 24, 2019.
Patel, Milan. Interview by Christopher D’Urso. In-Person, September 19, 2019.
Peguero, Carlos. “Opening Session.” Presented at the Council of Europe Octopus Conference on Cooperation Against Cybercrime, Strasbourg, France, November 20, 2019.
Poort, Tineke. “Male Captus, Bene Judicatus: Disguised Extradition and Other Practices.” *Leiden Journal of International Law* 1, no. 1 (1988): 65–77. https://doi.org/10.1017/S0922156500000686.
Prosecutor 2. Interview by Christopher D’Urso. Telephone, August 1, 2019.
Prosecutor 4. Interview by Christopher D’Urso. In-Person, August 6, 2019.
———. Interview by Christopher D’Urso. Video Call, March 31, 2021.

Prosecutor 6. Interview by Christopher D'Urso. In-Person, August 12, 2019.
Prosecutor 7. Interview by Christopher D'Urso. In-Person, August 12, 2019.
Prosecutor 9. Interview by Christopher D'Urso. Telephone, January 13, 2020.
Prosecutor 10. Interview by Christopher D'Urso. In-Person, August 9, 2019.
Prosecutor 11. Interview by Christopher D'Urso. In-Person, August 5, 2019.
Prosecutor 13. Interview by Christopher D'Urso. In-Person, August 8, 2019.
Prosecutor 14. Interview by Christopher D'Urso. In-Person, August 8, 2019.
Prosecutor 15. Interview by Christopher D'Urso. In-Person, August 14, 2019.
Prosecutor 17. Interview by Christopher D'Urso. In-Person, August 5, 2019.
Prosecutor 18. Interview by Christopher D'Urso. In-Person, August 8, 2019.
Prosecutor 20. Interview by Christopher D'Urso. In-Person, August 8, 2019.
Prosecutor 21. Interview by Christopher D'Urso. In-Person, September 17, 2019.
Prosecutor 22. Interview by Christopher D'Urso. In-Person, August 22, 2019.
Prosecutor 23. Interview by Christopher D'Urso. In-Person, August 16, 2019.
Prosecutor 24. Interview by Christopher D'Urso. In-Person, August 6, 2019.
Prosecutor 27. Interview by Christopher D'Urso. In-Person, August 13, 2019.
Prosecutor 28. Interview by Christopher D'Urso. In-Person, August 9, 2019.
———. Interview by Christopher D'Urso. In-Person, January 7, 2020.
Prosecutor 29. Interview by Christopher D'Urso. In-Person, August 13, 2019.
———. Interview by Christopher D'Urso. Video Call, March 19, 2021.
Prosecutor 30. Interview by Christopher D'Urso. In-Person, August 12, 2019.
Prosecutor 31. Interview by Christopher D'Urso. Telephone, August 16, 2019.
———. Interview by Christopher D'Urso. Telephone, September 16, 2020.
———. Interview by Christopher D'Urso. Telephone, March 15, 2021.
Prosecutor 32. Interview by Christopher D'Urso. In-Person, August 20, 2019.
Prosecutor 35. Interview by Christopher D'Urso. Telephone, August 21, 2019.
Prosecutor 38. Interview by Christopher D'Urso. Skype, August 20, 2019.
Prosecutor 39. Interview by Christopher D'Urso. In-Person, September 9, 2019.
Prosecutor 40. Interview by Christopher D'Urso. In-Person, September 9, 2019.
Prosecutor 41. Interview by Christopher D'Urso. In-Person, September 16, 2019.
Prosecutor 42. Interview by Christopher D'Urso. In-Person, September 4, 2019.
Prosecutor 44. Interview by Christopher D'Urso. In-Person, August 21, 2019.
Prosecutor 45. Interview by Christopher D'Urso. In-Person, September 9, 2019.
Prosecutor 47. Interview by Christopher D'Urso. In-Person, August 23, 2019.
Prosecutor 48. Interview by Christopher D'Urso. In-Person, September 5, 2019.
Prosecutor 49. Interview by Christopher D'Urso. In-Person, September 13, 2019.
Prosecutor 52. Interview by Christopher D'Urso. In-Person, September 20, 2019.
Prosecutor 53. Interview by Christopher D'Urso. In-Person, September 16, 2019.
Prosecutor 55. Interview by Christopher D'Urso. In-Person, September 4, 2019.
Prosecutor 57. Interview by Christopher D'Urso. Telephone, January 8, 2020.
Prosecutor 58. Interview by Christopher D'Urso. Skype, January 8, 2020.
Prosecutor 61. Interview by Christopher D'Urso. Telephone, October 1, 2020.
———. Interview by Christopher D'Urso. Telephone, December 3, 2020.
Prost, Kimberly. "No Hiding Place: How Justice Need Not Be Blinded by Borders." In *Combating International Crime: The Longer Arm of the Law*, edited by Steven David Brown, 123–62. London: Routledge-Cavendish, 2008.
"Public Trust in Banking." YouGov-Cambridge, April 2013. https://cdn.yougov.com/cumulus_uploads/document/ylf7gpof19/Public_Trust_in_Banking_Final.pdf.

International Law Commission. “Responsibility of States for Internationally Wrongful Acts,” 2005. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.
Reza, H.G. “Attorney Says Client Was Kidnaped; Wants Drug Charges Dropped.” Los Angeles Times, February 12, 1986. https://www.latimes.com/archives/la-xpm-1986-02-12-me-27585-story.html.
Rid, Thomas, and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37. https://doi.org/10.1080/01402390.2014.977382.
Rose, Cecily. “Treaty Monitoring and Compliance in the Field of Transnational Criminal Law.” *Brill Research Perspectives in Transnational Crime* 1, no. 2–3 (2017): 40–64. https://doi.org/10.1163/24680931-12340004.
Rosenstein, Rod. Interview by Christopher D’Urso. In-Person, September 17, 2019.
Rowe, Brenda I. “Transnational State-Sponsored Cyber Economic Espionage: A Legal Quagmire.” *Security Journal* 33, no. 1 (March 1, 2020): 63–82. https://doi.org/10.1057/s41284-019-00197-3.
U.S. Department of Justice. “Russian Computer Hacker Convicted by Jury,” October 10, 2001. https://www.justice.gov/archive/criminal/cybercrime/press-releases/2001/gorshkovconvict.htm.
U.S. Department of Justice. “Russian Man Sentenced for Hacking into Computers in the United States,” July 25, 2003. https://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/ivanovSent.htm.
Sadoff, David A. *Bringing International Fugitives to Justice: Extradition and Its Alternatives*. Cambridge, United Kingdom: Cambridge University Press, 2016.
Saugman, Frederick. “UK Courts Raise the Bar to US Extradition.” WilmerHale, August 10, 2018. https://www.wilmerhale.com/en/insights/blogs/wilmerhale-w-i-r-e-uk/20180810-uk-courts-raise-the-bar-to-us-extradition.
Scharf, Michael P. “Case Analysis: The Prosecutor v. Slavko Dokmanovic: Irregular Rendition and the ICTY.” *Leiden Journal of International Law* 11, no. 2 (1998): 369–82.
Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524.
Schroeder, Steve. *The Lure: The True Story of How the Department of Justice Brought Down Two of the World’s Most Dangerous Cyber Criminals*. Boston: Course Techology, 2012.
———. Interview by Christopher D’Urso. Video Call, April 2, 2021.
Seger, Alexander. “Opening Session.” Presented at the Council of Europe Octopus Conference on Cooperation Against Cybercrime, Strasbourg, France, November 20, 2019.
———. “Results of Capacity Building and Impact on Legislation.” Presented at the Council of Europe Octopus Conference on Cooperation Against Cybercrime, Strasbourg, France, November 20, 2019.
Senior English Barrister 1. Interview by Christopher D’Urso. Video Call, January 4, 2021.
Senior English Barrister 2. Interview by Christopher D’Urso. Video Call, January 5, 2021.
Shull, Aaron. “Global Cybercrime: The Interplay of Politics and Law.” Internet Governance Papers. Waterloo, Ontario: Centre for International Governance Innovation, June 2014.
Sinclair, Fergus. Interview by Christopher D’Urso. Telephone, January 5, 2020.

Soma, John, and Thomas Muther. “Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?” *Harvard Journal on Legislation* 34, no. 2 (1997): 317.

Sridhar, Aparna. “The International Criminal Tribunal for the Former Yugoslavia’s Response to the Problem of Transnational Abduction.” *Stanford Journal of International Law* 42, no. 2 (2006): 343–64.

Stansell-Gamm, Marty. Interview by Christopher D’Urso. Skype, October 7, 2019.

Stewart, David P. “The Emergent Human Right to Consular Notification, Access and Assistance.” In *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric*, edited by Andreas von Arnauld, Kerstin von der Decken, and Mart Susi, 439–52. Cambridge: Cambridge University Press, 2020. https://doi.org/10.1017/9781108676106.035.

Stigall, Dan. “Counterterrorism, Ungoverned Spaces, and the Role of International Law.” *The SAIS Review of International Affairs* 36, no. 1 (2016): 47–60. https://doi.org/10.1353/sais.2016.0011.

———. Interview by Christopher D’Urso. In-Person, August 15, 2019.

———. Interview by Christopher D’Urso. Telephone, November 4, 2020.

U.S. Department of Justice. “Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases (January 2009 to the Present: Updated May 13, 2015),” May 13, 2015. https://www.justice.gov/file/438491/download.

Voice of Ceylon. “Superpowers Fight It Out Over Russian Hacker in Colombo,” December 24, 2017. http://english.voiceofceylon.com/2017/12/24/superpowers-fight-russian-hacker-colombo/.

Thomson, Janice E. *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*. Princeton Studies in International History and Politics. Princeton: Princeton University Press, 1994.

U.S. Department of Justice. “Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe,” February 17, 2021. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

Travis, Alan, and Owen Bowcott. “Gary McKinnon Will Not Be Extradited to US, Theresa May Announces.” The Guardian, October 16, 2012. https://www.theguardian.com/world/2012/oct/16/gary-mckinnon-not-extradited-may.

U.S. Department of Justice. “Two Romanian Nationals Plead Guilty to Participating in Multimillion Dollar Scheme to Remotely Hack into and Steal Payment Card Data from Hundreds of US Merchants’ Computers,” September 17, 2012. https://www.justice.gov/opa/pr/two-romanian-nationals-plead-guilty-participating-multimillion-dollar-scheme-remotely-hack.

U.S. Department of Justice. “U.K. Computer Hacker Charged in Manhattan Federal Court with Hacking into Federal Reserve Computer System,” February 27, 2014. https://www.justice.gov/usao-sdny/pr/uk-computer-hacker-charged-manhattan-federal-court-hacking-federal-reserve-computer.

UN Office on Drugs and Crime. “Comprehensive Study on Cybercrime.” New York: United Nations, February 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

United Nations Office on Drugs and Crime. “United Nations Convention Against Corruption.” Accessed December 31, 2019. https://www.unodc.org/unodc/en/corruption/uncac.html.

U.S. Department of Justice. “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,” May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

U.S. Department of Justice. “U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts,” March 15, 2017. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

U.S. Department of Justice. “U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations,” October 4, 2018. https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

U.S. Department of Justice. “U.S. Leads Multi-National Action Against ‘Gameover Zeus’ Botnet and ‘Cryptolocker’ Ransomware, Charges Botnet Administrator,” June 2, 2014. https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

Verdelho, Pedro. “The Effectiveness of International Co-Operation against Cybercrime: Examples of Good Practice.” Discussion Paper. Strasbourg, France: Council of Europe Project on Cybercrime, March 12, 2008.

Wall, David. *Cybercrime: The Transformation of Crime in the Information Age*. Crime and Society Series. Cambridge: Polity, 2007.

Weinstein, Jason. Interview by Christopher D’Urso. In-Person, August 6, 2019.

———. Interview by Christopher D’Urso. Telephone, January 10, 2020.

Weiser, Benjamin. “Afghan Linked to Taliban Sentenced to Life in Drug Trafficking Case.” The New York Times, May 1, 2009. https://www.nytimes.com/2009/05/01/nyregion/01sentence.html.

Williams, Rob. “Computer Hacker Gary McKinnon Will Face No Further Action Says CPS.” The Independent, December 14, 2012. https://www.independent.co.uk/news/uk/crime/computer-hacker-gary-mckinnon-will-face-no-further-action-says-cps-8417875.html.

Yakovlev, Andrey. “The Dark Side of Russia: How New Internet Laws and Nationalism Fuel Russian Cybercrime.” IntSights, August 8, 2019.

Zetter, Kim. “Ukrainian Carding King ‘Maksik’ Was Lured to Arrest.” July 28, 2010. Wired. Accessed December 1, 2020. https://www.wired.com/2010/07/maksik-lured-to-arrest/.