The Failed Digital State Problem? Capacity Gaps and Managing Internet Externalities

Harry Oppenheimer,[1]

Updated: April 3, 2023

For the most current version of this paper please use the Dropbox link (https://www.dropbox.com/s/0sfvgbsaeinggg i/dns_data_externality_022123.pdf?dl=0)

Abstract: Do gaps in enforcement capacity worsen or alleviate the effect of interdependence on shared externalities? The internet enables much of the global economy, but there has been little investigation of how digital security interacts with the international system in a non-military context. In this paper, I lay out a theory of cyber threat networks that draws from the computer science literature on network security and focuses on digital interdependence. I hypothesize that greater interdependence between states at the infrastructural level will result in shared transnational digital threats. The policy community argues that this effect is exacerbated by differences in capacity within dyads, while I hypothesize that greater power differentials will also enable strong states to enforce standards in weaker ones. I test this with a cybersecurity engineering dataset of 40 million malware programs and internet interconnection agreements between over 100,000 internet service providers in 215 IP address spaces from 2015-2020, revealing how bilateral digital interdependence among internet operators generates shared risk from malware hosts and threats between states. This externality arises as non-governmental organizations network across borders, and cannot be explained by rivalry, conflict, or trade networks. Surprisingly, the effect of interdependence on shared threat is the strongest with small bilateral gaps in capacity. To explain this, I use a case study of Australia to demonstrate how larger gaps in capacity combined with asymmetric dependence in the internet's structure allow strong states to enforce standards. This paper contributes to the international political economy literature on digital trade and interdependence by bringing in network security and contributes to theories about how economic interdependence among non-state actors creates incentives for states to invest in regimes and cooperation.

Acknowledgments: I would like to thank Adam Breuer, Christina Davis, Iain Johnston, Joshua Kertzer, Gary King, Nadiya Kostyuk, Bruce Schneier, Dustin Tingley, and JD Work.

[1] PhD Candidate, Harvard University. 1737 Cambridge St, Cambridge MA 02138. Email: hoppenheimer@g.harvard.edu Web: https://scholar.harvard.edu/hoppenheimer.

1 Introduction

The internet is a highly interdependent global system that harnesses advances in communication technology to move information efficiently, inexpensively, and quickly. Threats to the internet are similarly global, and malicious actors use transnational host networks to target vulnerable systems, move information efficiently, and avoid detection. This paper uses forensic analyses of malicious program hosting to explore the connection between internet interdependence (how reliant two states are on one another to move data through the internet) and shared digital threat (how malicious actors use two states' digital infrastructure to host and deliver threats). Do interdependent states share greater digital threats, and do capacity gaps worsen or alleviate the impact of interdependence on shared threats?

While internet-driven globalization has created an era of massive economic and social advancement, the literature has yet to address how digital interdependence affects states or created incentives for digital security cooperation. Within political science cybersecurity threats are typically conceptualized through large-scale attacks with explicitly political or military goals. There are two models cyber threat threat, only one of which existing literature on cybersecurity considered. There are threats due to states exercising coercive measures to gain strategic advantage, and there are threats that millions of internet users face daily.

This paper explores this second model of threat – the larger phenomenon that occurs over 30 million times per year, cost the global economy $3 trillion by 2015, and is estimated to cost the global economy $10.5 trillion annually by 2025. An essential part of how threat actors target systems, and how defenders understand threats, is through malware hosting. This paper evaluates the effect of interdependence on whether malicious actors host threats between states. This co-hosting matters because threats leverage international borders to target systems. When countries co-host significant amounts of malicious programs, efforts to shut down hosts in one country improve security in the other, and states benefit more from sharing intelligence.

I examine how interdependent two countries are through internet interconnection agreements internet service providers negotiate to transfer data between digital systems, often across borders. This provides an accurate estimation for how dependent two countries internet infrastructures are on one another to connect with the global internet. I pair this interdependence data with digital forensic analysis geolocating the command and control servers for over 30 million malware programs discovered between May 2015 and December 2020. Through this we can understand when interdependence leads to shared threats, and whether this is intensified by capacity gaps.

One of the internet's defining characteristics is that it is an open system - internet users all interact with the same system, regardless of whether they are in states with low capacity interact or in states with high capacity. This fact motivates a persistent fear in the international community - hackers will use the internet space in low-capacity states to host and deliver attacks to users in high-capacity states. Policymakers and international organizations frequently argue that weak states or gaps in state capacity will exacerbate cybersecurity threats. If the internet brings about new interdependence, it may create spillover where users in wealthy countries with robust domestic security regulations are bombarded by threats from less wealthy countries without strong standards. However, this paper demonstrates that this simple model of externalities, where the level of shared threat is a function of the exposure between states and the difference in capacity between them, does not hold. Instead, differences in state capacity result in a *lower* effect of interdependence on shared threats.

I argue this counter-intuitive finding is because greater differences in capacity allow stronger states to dictate and coordinate policy in weaker states, resulting in deep cooperation not possible in bilateral relations between equally capable states. The explanation for this finding exists in the international relations literature on asymmetric dependence. Powerful states can leverage asymmetric dependence to shape rules and compel weaker states to adjust policies(Lake, 2009; Brooks and Wohlforth, 2008; Gilpin and Gilpin, 1987; Gowa, 1994). Several of the internet's more hierarchical features create dependency opportunities.

On the global internet, asymmetric interdependence is due to the structure of the internet and how new adopters must find existing partners who can facilitate their access to the rest of the network (Barabási and Albert, 1999; Chang, Jamin and Willinger, 2006; Clegg, Di Cairano-Gilfedder and Zhou, 2010). I demonstrate this dynamic with a case study of Australia in the South Pacific. Small island nations rely almost exclusively on Australia to facilitate access to the global internet architecture. Over the past ten years Australia has been able to shape the domestic cybersecurity institutions in each of these states, even as these states attempted to build closer digital relationships with China. These efforts include dictating strategy and policy and promoting new regulators and regulatory bodies. The result is a regional cybersecurity regime in the South Pacific where gaps in capacity under conditions of interdependence created the incentives and opportunity for a regional power to successfully invest in cooperation.

This paper continues as follows. First, it lays out a theory of cybersecurity drawing from the computer science literature, and demonstrates how computer scientists think of cybersecurity threat. Drawing on technical datasets, it demonstrates how cybersecurity threats are transnational phenomena representing shared challenges to interdependent states. Finally, it demonstrates how Australia created a cybersecurity regime with its regional partners in the South Pacific due to these concerns. The paper concludes with several considerations for future research on digital interdependence and cooperation, including potential free-riding on cybersecurity investments, diverging incentives to manage digital threat through multilateral or bilateral channels, and whether regulatory convergence may lead to increased internet interdependence.

2 Global Threat Networks

This paper introduces the concept of a threat network from computer science. Malware, a portmanteau for malicious software, is designed to exploit vulnerabilities in computers and networks with various methods. Hackers want to use malware to access and exfiltrate information from digital systems. Malware programs use command and control (C2) servers to remotely control and manage infected computers. This network allows attackers to execute commands, steal data, or install additional malware on the infected system. Malware hosts are analogous to safe houses for a criminal enterprise. Threat networks are collections of C2 servers that all work together to target systems - they are related because the same individual or organization leverages them to deliver the same threat.

One of the main ways programmers write and distribute malicious code is through the Domain Name System (DNS), a vital part of the application layer of internet protocol (TCP/IP). This system links domain names to hosts, but provides attackers with an agile way to command their malicious programs (Antonakakis et al., 2010). Hackers try to disguise their true intention by leveraging trusted hosts or creating degrees of separation to the endpoint so that they can rapidly move hosts when a server is blocked (Bilge et al., 2014). Researchers learn about patterns of malware-hosting by running viruses in a controlled environment and capturing packages using programs such as Wireshark (Antonakakis et al., 2011; Perdisci, Lee and Feamster, 2010; Rahbarinia, Perdisci and Antonakakis, 2016; Rieck et al., 2008). With enough programs, they can understand the URLs and IP addresses that hackers use to target systems. Defenders can block a new domain that connects to an IP hosting malware or a new IP address that connects to a malicious domain, and law enforcement agencies gather intelligence about potential criminal networks.

Despite our conception of cyberspace as borderless, malicious programs use distance and changes to avoid detection, and so how these programs map onto physical space can be used to identify whether programs have malicious intent. This includes characteristics of the host location, including the geographic diversity of hosts. Defenders leverage geographic diversity because malicious programs need to route DNS queries to a more diverse set of locations to avoid detection (Antonakakis et al., 2010; Perdisci et al., 2009).

Many threat networks are international and use servers in multiple countries as transnational networks. Table 1 contains the DNS resolutions for one hypothetical malware program.

The program delivered packets, or communicated, with 6 IP addresses via 6 domains in 6 countries. This program is a one link between the United States, Germany, India, the Czech Republic, Turkey, and Poland. The program's author may have been in any of these locations, or potentially in none of them. However, this hacker leveraged servers in these 6 countries, and it did so to exfiltrate stolen information and command their program. This could be a botnet in Turkey which uses servers in Poland, or a criminal network in Poland that uses servers in India. The key is that one or more computers in these 6 countries are being used at the same time to target systems, and are controlled to deliver the same type of threat.

Table 1: Example of Passive DNS Data for a Malware Program

MD5 Hash	Domain	IP Address	Country
e8961b7d769ae1bcb***	cart***.org	206.189.61.***	DE
e8961b7d769ae1bcb***	eskimo***.com	216.10.240.***	IN
e8961b7d769ae1bcb***	esou***.co.in	162.217.99.***	US
e8961b7d769ae1bcb***	fotbalba***.yc.cz	88.86.100.***	CZ
e8961b7d769ae1bcb***	fourl***.com.tr	185.126.217.***	TR
e8961b7d769ae1bcb***	ilo.br***.pl	148.81.111.***	PL

The table shows an example of the resolved domains in the Passive DNS analysis of one malware program. The first three columns of this data are produced by the Georgia Tech Information Security Center and available through the Impact Cyber Trust. This information is contained in one csv file with all the programs from the same day. The country information was added through ipstack, a private service providing WHOIS IP-lookup information.

Why does this matter for international politics? If threats are interdependent, countries' cybersecurity is interdependent. Shutting down any of the servers in Table 1 would force the malware program to switch command and control. Greater cybersecurity standards in one of these countries might result in fewer infected computers, which shrinks the supply of malicious program hosts. Nadji et al. (2013) demonstrate that disabling 20% of a criminal network's hosts reduces the overall success of the criminal network's hosting by 70%. The entire network becomes degraded if authorities disrupt one part of it.

To understand the implications of threat networks, consider some hypothetical scenarios. If Germany and the Czech Republic only appear in malicious programs together, they share significant digital threats. If Germany enacted new regulations and shut down servers that are used to co-host programs, the Czech Republic benefits. North Korea is not featured in any of these programs, indicating that programs are not using North Korean computers and systems to exfiltrate data to other countries. North Korea may be behind threats, but cybersecurity in the United States is not a function of cybersecurity in North Korea because the two countries have little to no shared digital risk. On the other hand, the US-based hosts frequently appear in programs with Dutch-based hosts, indicating that US cybersecurity is, to a large degree, a function of Dutch cybersecurity.

Emotet is one of the most prominent examples of a threat network that used parked domains to deliver payloads to attack systems around the globe. Emotet forced Allentown, PA to spend $1M on recovery in 2018[2] and compromised Lithuanian government systems in 2020.[3] In 2019 the forensic cybersecurity group Black Lotus Labs validated the identity of hundreds of Emotet command and control addresses. They found that the hosts were mostly located in the United States in Germany, but could also be found in Argentina, Colombia, Mexico, Ecuador, Pakistan, India, and South Africa.[4] The FBI estimated that over a ten-month period Emotet infected 1.6 million computers, including 45,000 in the United States. The operation to take down the network required a multinational operation involving the United States, Canada, France, Germany, the Netherlands, and the United Kingdom, and additional assistance from officials in Lithuania, Sweden, and Ukraine.[5] This is one example of a threat network - one actor using hosts in multiple countries to launch attacks. The question remains regarding where these networks are more or less dense, and how malicious actors create their hosting networks to deliver threats.

[2] Tung, Liam. "Microsoft: How One Emotet Infection Took out This Organization's Entire Network." *ZDNet*, April 3, 2020. https://www.zdnet.com/article/microsoft-how-one-emotet-infection-took-out-this-organizations-entire-network/.

[3] Damulytė, Jūratė, and Ignas Jačauskas. "Lithuania's Public Health Body Comes under Cyber Attack." *LRT English*, December 30, 2020. https://www.lrt.lt/en/news-in-english/19/1309469/lithuania-s-public-health-body-comes-under-cyber-attack.

[4] Lumen. "Emotet Illuminated: Mapping a Tiered Botnet Using Global Network Forensics," June 17, 2019. https://blog.lumen.com/emotet-illuminated-mapping-a-tiered-botnet-using-global-network-forensics/.

[5] Department of Justice. Press Release. "Emotet Botnet Disrupted in International Cyber Operation." *Press Release*, January 28, 2021. https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

3 Interdependence and Externalities

What determines the relative degree of shared cybersecurity threat between two countries? Shared cybersecurity risks are externalities, which Davis, North and Smorodin (1971) describes as "the fact that some costs or revenues are external to the decision-making unit" (p. 15). A core part of the extnernality model of cooperation is the idea that interdependence increases exposure to externalities (Keohane and Nye, 1973; Keohane, 1984).

Borders and distance, which may represent the interdependence between states, can often be a conduit for externalities or "spillover effects." For example, interdependence via geographic distance captures the effect of transnational spillovers such as technology or unemployment on economic growth (Conley and Topa, 2002; Ertur and Koch, 2006; Keller, 2002; Moreno and Trehan, 1997). Countries benefit from research and development spending in other states, where interdependence captures the intensity of those effects (Coe and Helpman, 1995).

Economic interdependence can lead to shared risks. Increasing international trade and regional integration led to the creation of to transnational crime networks (Schönenberg and von Schönfeld, 2013; Shelley, 1995), and greater exposure to credit risk during financial crises (Cheung, Fung and Tsai, 2010; Corsetti, Pericoli and Sbracia, 2005).[6]

The interdependence-digital risk framework is part of the cybersecurity discourse. The Council of Economic Advisers (2018), tasked with analyzing the future of the digital economy, wrote that "Cybersecurity is a common good; lax cybersecurity imposes negative externalities on other economic entities and on private citizens. Failure to account for these negative externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment" (2018, p.1). The authors of a RAND report on cybersecurity scaled this argument to the global level, that in a world of complex digital

[6] The claim that different states are interdependent at the internet-level is distinct the interdependence of different critical infrastructures. Many claim cybersecurity is important because societal functions are dependent on critical infrastructures, which rely on the internet to operate efficiently. For example, see Clemente and Royal Institute of International Affairs (2013). However, these are claims about the interdependence between society and the internet, rather than between the internet in two different societies.

threats, “a country’s ICT-enabled prosperity and well-being is becoming more and more dependent on the security and resilience of networks located well beyond its national borders and jurisdiction” (Bellasio et al., 2018, p. 1).

While transnational cyber threats are an increasingly dangerous phenomena, they are not new. Part of what makes cyberattacks particularly difficult to deal with is that they are cross-national and leverage distance from the target to avoid defensive measures. In 1991 John Markoff of the *New York Times* reported that “Beyond the reach of American law, a group of Dutch computer intruders have been openly defying United States military, space and intelligence authorities for almost six months.”[7] Even the most sophisticated attacks such as Stuxnet caused spillover effects for other systems and presented a shared digital risk - one type of threat affected users in multiple countries. It delivered a payload to a Siemens SCADA system using four zero-day exploits to damage Iranian nuclear centrifuges. The authors designed the program to be inert after a specific date and spread from one system to no more than three others. However, in the end STUXNET effected over 100,000 computers, of which 58% were in Iran, 17% were in Indonesia, 10% were in India, and 3.4% were in Azerbaijan.[8] However, it is not clear whether shared digital risk follows patterns of interdependence.

National cybersecurity strategies, which set policy priorities and express national views on cyberspace, have recognized that part of the unique challenge of digital threats are their transnational nature. This means that cooperation with other states has become central to cybersecurity plans. The U.S. *National Cyber Strategy* states that the country must “strengthen the capacity and interoperability of those allies and partners to improve our ability to optimize our combined skills, resources, capabilities, and perspectives against shared threats” (The White House, 2018, p. 26). Estonia’s *National Cybersecurity Strategy*

[7] Markoff, John. “Dutch Computer Rogues Infiltrate American Systems With Impunity.” *The New York Times*, April 21, 1991, sec. U.S.

[8] Falliere, Nicholas, Liam O Murchu, and Eric Chien. “W32.Stuxnet Dossier.” Cupertino, CA: Symantec Security Response, November 2010. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

(2014) lists among the challenges "In the case of vital services, cross-border information technology interdependencies have emerged and securing them is no longer dependent solely on parties based in Estonia" (p. 6).[9]

The cybersecurity and globalization narrative also makes it clear that interdependence a source of shared risks in cyberspace both in the bilateral and multilateral context. Lindy Cameron, CEO of the UK National Cyber Security Centre (NCSC), expressed the incentives for greater cooperation with Ireland. She stated in a speech announcing a new dialogue that "Given those cross-border dependencies in many CNI sectors, there is a particular cross-over in threats facing Northern Ireland and Ireland...cross-border transport links increases the potential for cyber attacks, including ransomware."[10] The European Union Directive on security of network and information systems (NIS) argues that "Owing to that transnational nature [of network infrastructure systems], substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole."[11]

While the literature argues that interdependence creates shared threat networks, and the global community fears that digital interdependence exposes countries to shared risk, this has not been addressed within the existing digital politics literature. Nye (2016) discusses entanglement in cybersecurity, arguing that digital interdependence creates a situation where the attacker will avoid exploiting an adversary system because they are unable to control the the consequences. However, digital interdependence may also shape the underlying network that hakcers use to target individual internet users.

Hypothesis 1: Controlling for traditional forms of interdependence, interdependence between internet infrastructures leads to shared digital threat.

[9] Estonia. "Cyber Security Strategy 2014-2017." Ministry of Economic Affairs and Communication, 2014.

[10] National Cyber Security Centre. "Lindy Cameron Speaking to the IIEA," June 25, 2021. https://www.ncsc.gov.uk/speech/iiea-cyber-threat.

[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Pub. L. No. 32016L1148, OJ L 194 (2016). http://data.europa.eu/eli/dir/2016/1148/oj/eng.

How is the effect of greater interdependence on shared cybersecurity threats between states moderated by differences in state capacity? The contagion model provides one clear hypothesis - that low capacity and crises in one area will spread to another as interdependence increases (Patrick, 2007). This dynamic is a large part of the post-Cold War security discussion. President George Bush noted in the 2002 *National Security Strategy* "America is now threatened less by conquering states than we are by failing ones." The 2006 National Security Strategy of the United States stated that "Weak and impoverished states and ungoverned areas are not only a threat to their people and a burden on regional economies, but are also susceptible to exploitation by terrorists, tyrants, and international criminals." Ambassador Karl Ikenberry (2015) argued that failing or failing states are a problem due to "contagion, or the transmission of threats from one weak state to another."

The literature on conflict spillovers often argues that weak states create negative security externalities for their neighbors (Atzili, 2007; Beardsley, 2011; Metternich, Minhas and Ward, 2017). Buhaug and Gleditsch (2008) find that civil wars diffuse depending on the ethnic ties in neighboring states, while Salehyan and Gleditsch (2006) argues that conflict spills over within regions due to refugee flows and the transnational illicit flows that follow them. In these models, the level of negative externality is both a function of interdependence and capacity differences in multiple states.

Criminal networks provide a direct comparison for malware hosting networks. The literature on international criminal activities often identifies interdependence and enforcement gaps working in tandem to produce crime networks (Findlay, 2000; Naylor, 2004; Williams and Vlassis, 2001). Simmons, Lloyd and Stewart (2018) demonstrates how fear of negative externalities due to a neighbor criminalizing human trafficking leads states to adopt anti-human trafficking laws as criminal networks to shift and exploit the relative difference in capacity. The authors' mechanism is that interdependence, as measured by road networks, is a necessary step for legal gaps to result in criminal network shifts.

The idea that capacity gaps that allow attackers safe haven is enshrined in consensus international reports on cybersecurity. The United Nations has convened a Group of Government Experts Report (GGE) five times to discuss norms and principles for cyberspace. In 2013 the group produced a report that was unanimously adopted by the 18 national representatives, including the permanent five security council members. The report noted that "Different levels of capacity for ICT security among different States can increase vulnerability in an interconnected world. Malicious actors exploit networks no matter where they are located. These vulnerabilities are amplified by disparities in national law, regulations and practices related to the use of ICTs."[12]

The risks of low-capacity states for the international digital ecosystem also motivates the international capacity building agenda. At the United Nations experts have argued that their states should address gaps to prevent digital threat contagion. The 2015 GGE affirmed this, stating that "Providing assistance to build capacity in the area of ICT security is also essential for international security, by improving the capacity of States for cooperation and collective action."[13] The 2021 UN GGE report wrote that "In a digitally interdependent world, the benefits of capacity-building radiate beyond the initial recipients, and contribute to building a more secure and stable ICT environment for all." The Cybersecurity Tech Accord, made up of the largest international technology firms including Microsoft, facebook, and SAP, argues that addressing cybersecurity capacity gaps has both wide consensus and is necessary to ensure cyberspace stability.[14]

Hypothesis 2: The effect of internet interdependence on shared threat will be greater between states with larger gaps in capacity.

States have positive incentives to cooperate on regulatory and economic issues to manage their shared interests (Drezner, 2008), although this may depend on the type of externality

[12] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Pub. L. No. A/68/98* (2013).

[13] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Pub. L. No. A/70/174 (2015). https://undocs.org/pdf?symbol=en/A/70/174.

[14] Ciglic, Kaja. "Cybersecurity Capacity Building: A Foundational Element of International Peace and Stability Online." Cybersecurity Tech Accord (blog), March 24, 2021. https://cybertechaccord.org/cybersecurity-capacity-building-a-foundational-element-of-international-peace-and-stability-online/.

and home benefits and costs for states (Cooper, 1986) or for actors within states (Milner, 1997). The particular policy challenges associated with cybersecurity, including threat intelligence sharing, global standards, and transnational crime, make international cooperation essential. One of the internet's main features - preferential attachment - create a situation where low-capacity states are heavily dependent on high-capacity states for data transit. While gaps in capacity under conditions may expose high-capacity states to spillover from low-capacity states, cooperation may be more likely with capacity gaps where stronger states can enforce deeper cooperation.

Both states and the international community believe that cooperation will help limit shared threat, and international cooperation on cybersecurity measures is often justified on these grounds. Policy dialogues recognize that "securing cyberspace is a global challenge—one that cannot be solved by a single company or country on its own" (EastWest Institute, 2012). The 2013 Group of Government Experts Report noted that "Numerous bilateral, regional and multilateral initiatives since 2010 highlight the growing importance accorded to greater security of and in the use of ICTs, reducing risks to public safety, improving the security of nations and enhancing global stability." The 2021 UN GGE report stated "Ensuring an open, secure, stable, accessible and peaceful ICT environment requires effective cooperation among States to reduce risks to international peace and security."

The importance of cooperation for cybersecurity has also been expressed through national strategy documents. The *National Cybersecurity Strategy* states, "as a highly connected nation, the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners" (2017). Table 2 contains a few examples of international cooperation within national cybersecurity strategies. In cases such as Bermuda, the strategy outlined the specific countries and organizations with which they would seek cooperation. These statements are often placed in the context of the borderless nature of the internet and the idea that no one country can ensure effective cybersecurity without assistance from others.

Table 2: Doctrines Discussing International Cooperation

Country	Quote
Albania (2015)	Cyberspace as a borderless space requires international cooperation and coordination to ensure cyber security.
Bermuda (2019)	There is also recognition of the need for international cooperation with partners such as the National Crime Agency (NCA) in the United Kingdom and the Federal Bureau of Investigation (FBI) in the USA for best practices.
Jamaica (2015)	Additionally, it is recognized that the trans-border nature of cybercrime requires international cooperation to assist in the prosecution, mitigation and recovery efforts.
Estonia (2014)	Cyber security is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cybersecurity and enhances its own competence.
Netherlands (2013)	In view of the fact that cyber security and international cooperation are inextricably linked, the Netherlands will promote its integral public-private cyber security approach outside its own borders.
Serbia (2017)	Bearing in mind that cybercrime, due to the global reach of the Internet, knows no boundaries, it is extremely important to further improve international cooperation with the relevant foreign countries bodies.

Cooperation has already emerged in cyberspace, including threat information sharing frameworks between the United States and Japan,[15] Russia and China,[16] within the European Union,[17] and between 22 states in the Gulf Region.[18] These agreements are justified on the grounds that they will improve internet security for both parties. For instance, the U.S.-Japan agreement "recognized that the security and resilience of cyberspace can only be fully achieved through close cooperation and collaboration."

It is important to note that there is a tension between the different arguments laid out

[15] U.S. Department of State. "Joint Statement of the Uapan-U.S. Cyber Dialogue," July 24, 2017. https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Bilateral/Joint+Statement+of+the+Japan-U.S.+Cyber+Dialogue+7-24-2017.pdf.

[16] Government of the Russian Federation. "On Signing the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in Ensuring International Information Security," April 30, 2015. https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf.

[17] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Pub. L. No. 32016L1148, OJ L 194 (2016). http://data.europa.eu/eli/dir/2016/1148/oj/eng.

[18] ITU. "Oman ITU-Arab Regional Cybersecurity Centre." Accessed November 8, 2021. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.aspx.

here. Both the international community and international relations literature recognize that interdependence creates shared threats, gaps in capacity creates risk for capable countries, and that cooperation can lessen shared digital threat. However, if cooperation occurs "when actors adjust their behavior to the actual or anticipated preferences of others, through a process of policy coordination" then power imbalances allow states to more effectively force cooperative behavior (Keohane and Nye, 1973).

Power imbalances are precisely why some authors argue the rise United States as a hegemonic power is necessary to explain the emergence of the liberal international order (Kindleberger, 1973; Lake, 2009). In international political economy, unequal wealth in bilateral trade relations (Gowa, 1989; Oneal, Oneal, Maoz and Russett, 1996; Pollins, 1989; Gilpin and Gilpin, 1987) or greater importance within the international trading system may boost a state's ability to coerce others via sanctions (Drezner, 2015; Feaver and Lorber, 2010). When states are asymmetrically interdependent they are more likely to see effective conditionality (Baldwin, 1985; Drezner, 2003).

The technical structure of interconnection and the internet creates opportunities for asymmetric digital interdependence. There has been a significant amount of debate within the networks literature regarding whether the internet presents a hierarchical or mesh structure. The Barabasi-Albert model (1999) is the most well-known attempts to describe the internet network, which the authors argue is characterized by high levels of preferential attachment and growth over time. Preferential attachment, also known as "the rich get richer", is the concept that new nodes to the system prefer to join already well-connected nodes (Merton, 1968). In this case, a new internet service provider in a developing country would seek connections with a well-connected internet service provider within its nearby network. Due to the infrastructural demands of the internet, this may not be the most connected internet service provider, but rather one that can facilitate its access to the outside world. Several authors have demonstrated that autonomous systems display this behavior (Chang, Jamin and Willinger, 2006; Chen et al., 2002; Subramanian et al., 2002).

The Barabasi-Albert model has been debated within the networks literature as local data peering became more common (Dhamdhere and Dovrolis, 2010). However, authors debating the degree of digital preferential attachment typically make claims about networks with opportunities for partners, not networks along the internet's periphery.

Hypothesis 3: The effect of interdependence on shared threats will be less with larger gaps in capacity due to asymmetric interdependence.

This paper demonstrates how international internet interconnection system generates significant externalities, which states shares with others they are heavily networked with. First, I define the nature of digital threat, and explain how computer science deals with a different set of problems than the political science literature. Drawing on computer science perspective, I then demonstrate how greater digital interdependence creates shared externalities in digital threat. Returning to our understanding of how asymmetric interdependence facilitates top-down cooperation, I show how interdependence manifests in digital regimes between powerful states and their dependent neighbors.

4 Malware Hosting in Threat Networks

Because modern societies are highly dependent on digital systems, threats to these digital systems can be extremely costly. However, understanding the implications of increasing interdependence on shared threat requires several technical datasets that have never been leveraged within political science. Private technology firms collect much of the most sophisticated data on cyber threats. The cybersecurity market is valued at over $150 billion. These firms have a vast global network of computers with anti-virus software that informs them when attacks are occurring. Several papers have used data from these firms to understand threat patterns. Garg (2012) leveraged data from Microsoft and perspectives from criminal science to understand cross-national variation in the rates of computer infection. Microsoft does not publish the detailed data that Garg (2012) leverages, but they do produce several public reports.[19] Mezzour, Carley and Carley (2014) uses data from Symmantec's World Intelligence Network Environment (WINE) Intrusion Prevention System (IPS) to map out the factors contributing to cross-national malware threats.

Georgia Tech publishes the most significant publicly available cybersecurity dataset, the daily Passive DNS dataset, from May 2015 to the current day.[20] This dataset contains a daily average of 412,000 unique malware programs with at least one successful DNS resolution. Appendix Table **??** contains the number of programs analyzed per day. An earlier version of this dataset was used in 2010 to help Spanish and American law enforcement take down a global botnet that had infected 13 million machines in 190 countries.[21] This version was also used to create a reputation system for domain names (Antonakakis et al., 2010). This dataset contains some of the most famous malware families, including samples of the Wannacry ransomware attack that affected over 200,000 computers in 150 countries.

The engineers at Georgia Tech use a computer with limited access to the internet to run a suspected malicious program and collect information using a packet analysis program such as Wireshark. The analysis program collects information about cross-server communication including domain traffic and the IP addresses that the domains resolve to. To add additional information, I purchased an API access key for a WHOIS lookup service to convert these IP addresses into locations for each IP address. The result is a dataset of malware programs with the domains queried, the IP address each domain resolved to, and detailed information about the IP address such as where it is located in the world.

The key concept at the program-level is "how likely is it that a malware program queries domains located in two different countries at the same time?" This is a program which was written by one actor which is leveraging two servers to command and control the program. To formalize this, consider a series of malware programs named by their hash value $(MD5_i)_{i=1}^{\infty}$,

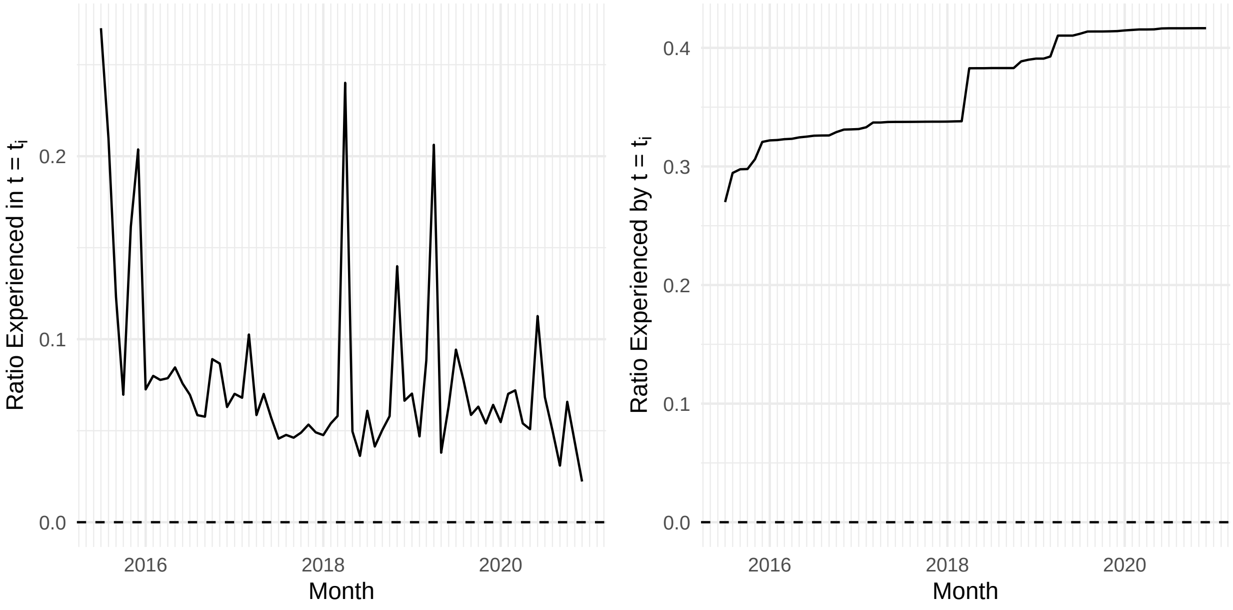
[19] Microsoft. "Microsoft Digital Defense Report and Security Intelligence Reports." Accessed September 27, 2021. https://www.microsoft.com/en-us/security/business/security-intelligence-report.

[20] [Georgia Tech] (N.d.)

[21] Higgins, Kelly Jackson. "Another Botnet Gets Dismantled, But This Time With Arrests." Dark Reading, March 5, 2010. https://www.informationweek.com/security/attacks/another-botnet-gets-dismantled-but-this/223101695.

where each program leverages an undirected network of IP addresses length n where $(H_i)_{i=1}^{n}$ which is hosted within some jurisdiction. By using the DNS system each host H is assigned a domain D.

In 2020, there are 249 countries of territories that are at risk for malware hosting based on the areas that are allocated IP address space by the Internet Assigned Numbers Authority (IANA). This includes the 193 sovereign countries with UN membership, along with several non-sovereign territories[22] and unoccupied territories.[23] This results in 30,876 undirected dyads that can have a malware program that is co-hosted. This is an extremely conservative estimate of the potential dyads at risk, since it includes dyads such as Antarctica-North Korea, or malware co-hosting with the Pitcairn Islands, which fewer than one billionth the number of IP addresses as the United States.



(a) Monthly Ratio

(b) Cumulative Ratio

Figure 1: Proportion of All Dyads Experiencing Co-Hosted Malware

Figure 1a presents the proportion of all dyads at risk that experience at least one co-hosted malware program in each month period, and Figure 1b presents the proportion of all dyads at

[22] For example, the Isle of Man, Mayotte, and the U.S. Virgin Islands

[23] For example, Antarctica and Heard Island

risk that have experienced at least one co-hosted malware program by the month in question. The monthly proportion of all dyads that experienced at least one malware program with hosts in both countries (1a) ranged from .022 (687 of 30876) in December 2020 to .269 (8335 of 30876) in July 2015. The cumulative proportion of unique dyads that experienced at least one co-hosted malware (1b) in the first month of observation was 0.269 and increased to 0.417 by the end of the observations. By December 2020, 12,862 of the 30,876 total dyads had featured at least one co-hosted malware program, where the hacker called hosts in both countries to launch the same threat.

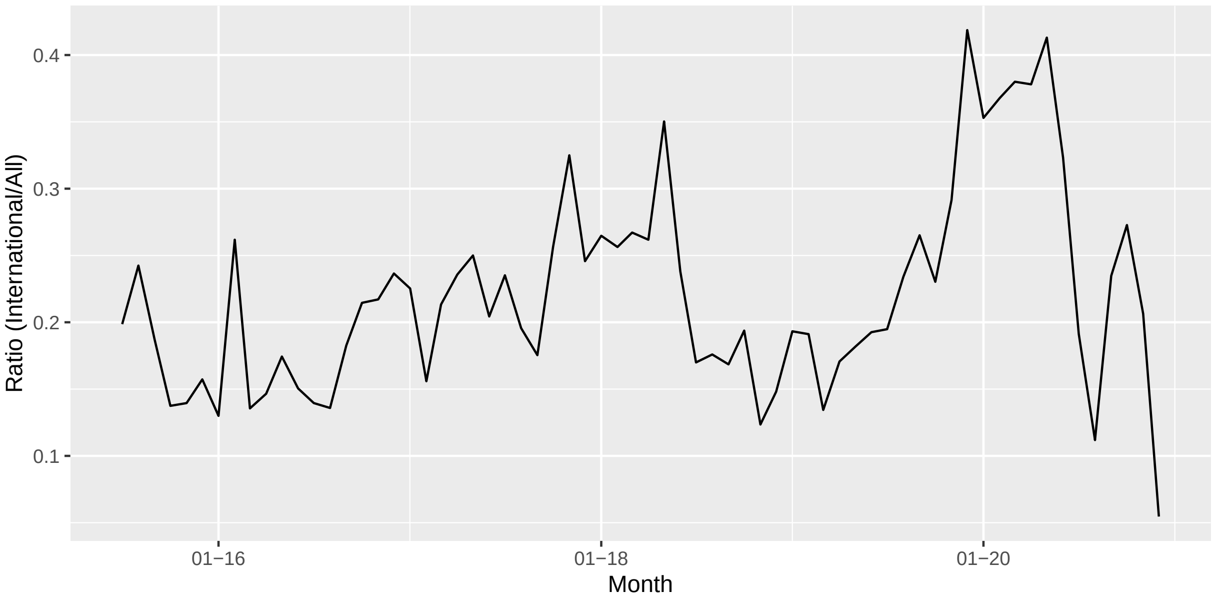
Figure 2 contains the ratio by month of programs that were utilized hosts in more than one country to all programs analyzed with at least one DNS resolution. The week of October 25, 2020 was the period with the highest ratio of domestic programs when 61,112 of the 116,446 programs had hosts in more than one country. The week of December 13, 2020 was the period with the highest ratio of international programs when 209,165 of the 215,374 programs had hosts in more than one country. When programs do not link internet spaces they tend to cluster in a few countries. At the monthly level, between 32% and 94% of the malware programs that leveraged hosts in only one country were in the United States. Furthermore, the 10 countries with the most single-country-hosted malware programs (United States, Poland, the Netherlands, China, Germany, Ireland, Russia, Hong Kong, Great Britain, and Luxembourg) represent 91.7% of all programs that leveraged hosts in one country.

5 Understanding Shared Digital Threat

5.1 Dependent Variable: Shared Threat

Leveraging Georgia Tech's passive DNS dataset, I build a time-series-cross-sectional dataset of the number of co-hosted malware programs between each pair of countries within a given month. For instance, in the matrix provided, at one given time there are a series of unique $MD5$ values, each with a series of hosts, and domains that link to the host. If H_1 and H_2

Figure 2: Ratio of International Programs to Total Programs



are in different countries, this can be thought of as a link between the internet space in the states at the level of the malicious program. This paper focuses on the program-level use of domains in different countries, but it may also be the case that the domains themselves switch across jurisdictions following patterns of peering as well.

$$\begin{bmatrix} t_1 & MD5_{1,1} & C_1 \\ t_1 & MD5_{1,1} & C_2 \\ t_1 & MD5_{1,2} & C_1 \\ t_1 & MD5_{1,2} & C_1 \\ t_1 & MD5_{1,2} & C_2 \\ t_1 & MD5_{1,3} & C_1 \\ t_1 & MD5_{1,3} & C_1 \end{bmatrix} \xrightarrow{Adjacency} \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \xrightarrow{TSCS} \begin{bmatrix} t_1 & C_1 & C_2 & 2 \end{bmatrix}$$

This measures the level of shared threat between each country on the internet, focusing on the bilateral links between control servers in each country. It is not just that the program is hosted in both countries, but that the hosts are themselves related because they are leveraged to execute one threat. One caveat is that this does not measure the origin source of the malicious program, which could be any of the nodes along the chain or may not be present at all. Instead, it is measuring the set of servers that are being used to control the program. While this data is collected at the day-level, I aggregate to the month level to match the main independent variable in the study, interconnection between each country. This data is modeled as undirected dyads, or the number of programs discovered with hosts in country a and country b in a month t.

5.2 Independent Variables

Economic Interdependence Interconnection may be technical, but it may also reflect existing economic and trading networks. Trade is also considered one of the most vital sources of interdependence in the international system. I use Comtrade data on the level of product trade between each state, which I aggregate from the two-digit level to the total bilateral trade per year. This data is provided by the Harvard Growth Lab and Center for International Development *Atlas of Economic Complexity*.[24] Alternatively, technology trade may provide a more accurate way of measuring interdependence and externalities for digital threats. The United Nations Conference on Trade and Development makes bulk data on bilateral trade flows for information communications technology (ICTs) available for 2000 through 2020. Since the malware and interconnection data are both undirected, I measure bilateral trade as the sum of exports between two countries, which is the same in each direction.

Relative Capacity If cybersecurity externalities are similar to the failed state problem, greater differences in state capacity may increase the presence of shared threat. I measure state capacity I use the World Bank *Worldwide Governance Indicators*, which includes 215 countries and territories (Kaufmann, Kraay and Mastruzzi, 2010). Most governance indicators, including Polity and Varieties of Democracy, do not have as wide a geographical scope. I use the "Government Effectiveness" index, which measures the quality of public services, civil service, policy formulation and implementation, and the credibility of government

[24] https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/T4CHWJ

policy. These indicators are measured as standard units. At the dyadic level I measure the difference in absolute value between the capacity of the two states.

Technical Interdependence To move information to between end-users the internet forms separate networks, known as autonomous systems (AS). How that individuals access the internet through an AS can shape the way that they interact with the wider internet, and provide governments with the opportunity to regulate internet exchanges (Lessig, 1999). An autonomous system (AS) refers to a network or group of networks that are controlled by a common administrator. In the earliest ASes were the universities and research institutions which formed the original nodes in ARPANET.[25] The number of systems increased from fewer than 5,000 in 1998 to over 70,000 in 2020.[26] Data can be exchanged between two systems AS organizations sign agreement - these organizations may be either in the same country or across national borders.

Zhuo, Huffaker, Claffy and Greenstein (2021) measured interstate internet integration through peering arrangements between Autonomous Systems (ASes) such as Internet Service Providers (ISPs). The authors find that privacy regulations have no impact on the number of international interconnection agreements between service providers. D'Ignazio and Giovannetti (2009) leverage interconnection agreements to understand the market power of different ISPs. The literature has not addresses whether non-state actors such as ASes choose whether to sign interconnection agreements based on the potential for harmful program hosting.

The Center for Applied Internet Data Analysis (CAIDA) at the University of California, San Diego gathers data about different aspects of the internet architecture. This paper leverages two CAIDA datasets, *AS Relationships* with peering agreements between systems,[27] and *AS Organizations* that maps autonomous system (AS) numbers to organizations.[28] These independent operators form agreements to exchange data between one another through

[25] For instance, Carnegie Mellon University owns AS9, the DoD Network Information Center owns AS13, and the Lawrence Livermore National Laboratory owns AS 44.

[26] Bates, Tony, Philip Smith, and Geoff Huston. "CIDR Report." Cidr. Accessed September 27, 2021. https://www.cidr-report.org/as2.0/.

[27] https://www.caida.org/data/as-relationships/

[28] https://www.caida.org/data/as-organizations/

the Border Gateway Protocol (BGP). This protocol is how my request for information on one system is routed to its destination. Organizations such as CAIDA place monitors that gather data about how data is routed, and, by extension, these independent operators agree to exchange data.

Internet monitors attempt to contact hosts and record information about how their connection is routed through the network. CAIDA leverages an algorithm to infer the type of agreement that the network operators are engaging in (Giotsas et al., 2013). Data can be exchanged in two different ways - either peer-to-peer (P2P) or provider-to-customer (P2C). This paper focuses on provider-to-customer agreements, since these are subject to less measurement error (Zhuo et al., 2021). The CAIDA data covers interconnection throughout the period covered in the Georgia Tech Passive DNS Dataset. I merge the interconnection agreement data with AS-to-Organization data and summarize interconnection at the monthly level to create a variable for the number of P2C agreements between each pair of countries (j_i, j_{-i}) in any given month (t). This provides me with a monthly measure of the level of interconnection between each territory registered within a regional internet registry.[29]

Other Coviariates

Rivalry While shared digital threat may be due to positive forms of interdependence, it may also result from adversarial relationships between states. One of the most discussed findings in the cybersecurity literature is the idea that cyber conflict is driven primarily by rival states (Valeriano and Maness, 2015). Rivalry may also increase externalities by preventing cooperation. I use the *Peace Data* on rivalries (Diehl, Goertz and Gallegos, 2019). Version 2 of the dataset covers rivalries through 2015. It codes adversarial relationships between states on a scale of "severe rivalry," "lesser rivalry," and "negative peace." For each country, I measure the number of countries with "severe rivalry" in each year. These are relationships "in which the sates see one another as enemies and competitors," and includes relationships such as India-Pakistan and US-Iran.

[29] See Appendix for more information regarding how this data was collected, cleaned, and aggregated.

Borders and Distance It may be the case that the architecture of the internet here is simply picking up the distance between countries and their borders. Countries share policy externalities due to geography. I measure this with contiguity and the distance between two countries in hundreds of kilometers (logged). The measures of distance and contiguity are from the *Dynamic Gravity Dataset*, which provides annual data for countries and country-pairs for 285 countries and territories (Gurevich and Herman, 2018). This measure of geographic distance is derived from (Zignago and Mayer, 2005), and takes into account the distance between pairs of cities weighted by population across countries. While many consider the internet to be "borderless," the internet has a physical infrastructure that may influence how data is exchanged. All else equal, there should be more data exchanged between two places that are closer to one another than two that are further away. This could be because greater distances may necessitate more expensive pieces of infrastructure, such as undersea submarine cables.

5.3 Methods

To understand the phenomenon of malware hosting I leverage a series of gravity models, which are a common econometric tool in the study of trade (Anderson, 2011; Carter and Poast, 2020), migration (Karemera, Oguledo and Davis, 2000), and urban planning (Erlander and Stewart, 1990). In the canonical gravity model, the imports between country a and country b are a function of the size of the two country's economies and a term to capture the cost of trading between the two countries. This cost is often measured as distance, but can also be border walls, similarities in regulatory regimes, or rivalry. Instead of measuring trade flows, I model the number co-hosted malware programs between two countries as a function of the number of interconnection between Autonomous Systems in the two countries, along with other factors which might traditionally suggest interdependence. Both co-hosting and interconnection agreements can occur between each of the 249 IP spaces, or 30,876 potential dyads.

This data is in an undirected dyad format, where the dependent variable the logged number of malware programs and estimated via linear models. I include country-year fixed effects to measure the time-varying country-level factors that might unilaterally affect a country's malware hosting, such as its internet speed, the number of internet users, or one state's capacity (Anderson, 2011; Baldwin and Taglioni, 2006). I do not include dyadic fixed effects in the models, since such a measure would answer whether increases or decreases in interconnection within a dyad results in increases or decreases in malware co-hosting. Instead, the quantity of interest is whether a country's malware co-hosting is a function of the countries that it is most interconnected with. I cluster standard errors at the dyad-level to help account for the correlation between dyadic observations across time periods.

$$ln[Malware_{i,j,t}] = \alpha_i + \alpha_j + \alpha_t + \beta_k X_{i,j,t,k} + \epsilon_{i,j}$$

In the formula above, the amount of shared malware between country i and country j in time t will be equal to fixed effects for country i and country j and time t and regressors k for pair i, j at time t and an error term for pair i, j. These regressors k can be the distance between i and j, the amount of interconnection between them, the amount they trade, if they share borders, or any other relationship we can measure between them.

6 Results

Table 3 contains the first set of results, including the base model along with varying controls. The coefficients in the table model the amount of shared digital threats between two countries. For a given country, the amount of shared digital threat that they face with each other country is a function of the relevant covariates. Because these models do not include dyadic fixed effects, they do not measure whether an increase in the amount of interdependence between two countries is associated with an increase in the level of shared digital threat, but whether the level of shared digital threat that they face with any given country is a function of their interdependence with it.

Table 3: Technical Interdependence and shared digital threat

Dependent Variable:	Shared Digital Threats					
Model:	(1)	(2)	(3)	(4)	(5)	(6)
Variables						
# Internet Interconnection Agreements	0.840***	0.839***	0.828***	0.481***	0.840***	0.475***
	(0.025)	(0.025)	(0.025)	(0.026)	(0.025)	(0.026)
PTA Agreement		0.014				-0.013
		(0.012)				(0.012)
Goods Trade			-0.019***			-0.023***
			(0.001)			(0.001)
ICT Goods Trade				0.318***		0.322***
				(0.008)		(0.008)
Rivalry					-0.022	-0.120
					(0.194)	(0.202)
Contiguity	-0.434***	-0.438***	-0.401***	-0.420***	-0.433***	-0.383***
	(0.055)	(0.056)	(0.057)	(0.053)	(0.058)	(0.056)
Distance	0.004	0.006	-0.031***	0.061***	0.004	0.026***
	(0.005)	(0.005)	(0.007)	(0.005)	(0.005)	(0.006)
Fixed-effects						
Country *a*	Yes	Yes	Yes	Yes	Yes	Yes
Country *b*	Yes	Yes	Yes	Yes	Yes	Yes
Month	Yes	Yes	Yes	Yes	Yes	Yes
Fit statistics						
Observations	1,753,290	1,753,290	1,417,218	1,546,776	1,753,290	1,395,900
R^2	0.45527	0.45530	0.47171	0.53707	0.45528	0.54339
Within R^2	0.17929	0.17933	0.17966	0.28701	0.17929	0.28988

Clustered (pair) standard-errors in parentheses

*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*

Model 1 shows that there is a relatively strong relationship between the technical interdependence between states and the level of shared digital threats between them. Since co-hosted malware is a logged variable, every 1% increase in the number of interconnection agreements is associated with a 0.84% increase in the number of co-hosted malware programs. The range of this dependent variable is 0 to 2172, and so the marginal effect of interdependence depends on the value of the independent variable. A marginal increase of 1 agreement from 1 to 2 agreements (100%) would indicate a 84% increase in shared digital threat, while a marginal increase of 1 agreement from 49 to 50 agreements (2%) would indicate a 1.62% increase in shared digital threat. Models 2-6 include alternative controls that may either contribute to shared digital threat, including whether the countries have a preferential trade agreement (2), the value of goods trade between them (3), the value of information communications technology trade between them (4), and whether they are rivals (5). Model 6 includes all of these controls at once. The sample sizes change due to missingness in the data on goods trade and ICT-specific goods trade. The association between technical internet interdependence and shared digital threat remains positive and statistically significant across each of the potential controls. Given this, I have a high degree of confidence that the amount of digital interdependence between two states is associated the degree of shared digital threats they face.

State-directed hacking attempts often follow patterns of rivalries (Valeriano and Maness, 2015). However, transnational digital threats also occur between sub-state actors in rival states. For instance, there is a long-running series of hacks between non-state actors in India and Pakistan. In 2017, a group of "patriotic hackers" from Pakistan claimed responsibility for hacking and defacing the websites of ten Indian universities. During independence celebrations in 2020, Indian hackers targeted over 80 Pakistani websites.[30] However, Models 5 and 6 in Table ?? demonstrates that rivalry is not a significant predictor of co-hosted

[30] "Indian Hackers Give Befitting Reply to Pakistan's Agenda on Ram Temple, Kashmir; Hack over 80 Pakistani Websites." Zee News, August 18, 2020. https://zeenews.india.com/india/indian-hackers-give-befitting-reply-to-pakistans-agenda-on-ram-temple-kashmir-hack-over-80-pakistani-w
html.

malware.

Digital interconnection between two countries or territories represents a distinct dimension of interdependence. An emerging literature has attempted to characterize data flows along with traditional forms of trade (Lopez Gonzalez and Ferencz, 2018). While internet interconnection agreements are highly correlated with data flows, they are a more fundamental part of the structure of the internet. Specifically, these agreements become part of the Border Gateway Protocol (BGP), which makes decisions on how data is routed between points on the internet. The protocol seeks to find the most efficient way to route data. Where there is interconnection there will be more reliable and robust data exchange.

The analysis thus far has demonstrated the first claim that the international community, state policies, and international relations literature all make - states face security and regulatory challenges with other states depending on how interdependent they are. Just as two states that trade trade frequently may face policy externalities, states with highly interdependent internet infrastructures face shared digital threats. However, does the effect of interdependence on the level of shared effect vary depending on differences in capacity across states, as many in the international community argue?

Table 4 contains the results for the differences in capacity across countries, both with and without an interaction between differences in capacity and internet infrastructural interdependence. In both models, differences in capacity are associated with less shared digital threat. Because government effectiveness is measured as standard units, differences in capacity are a half absolute normal distribution with $d \in [0, 4.7]$. A one unit increase in the relative capacity between two states is associated with a (exp(-0.160) - 1) * 100 = 14.6% decrease in the shared digital threat between them. A one-unit difference is roughly equal to Italy and Ukraine or the United States and Uruguay. Controlling for digital interdependence, larger gaps in capacity are associated with less, not more, shared threats.

Cyber criminals may use command and control servers in countries with lower capacity to fight cyber crime, and so each connection between ASNs across countries with capacity

Table 4: Relative capacity and shared digital threat

Dependent Variable:	Shared Digital Threats	
Model:	(1)	(2)
Variables		
# Internet Interconnection Agreements	0.807***	0.979***
	(0.024)	(0.034)
Difference in Capacity	-0.1601***	-0.136***
	(0.006)	(0.006)
# Interconnection Agreements × Difference in Capacity		-0.191***
		(0.026)
Contiguity	-0.449***	-0.512***
	(0.054)	(0.055)
Distance	0.019***	0.017***
	(0.005)	(0.005)
Fixed-effects		
Country *a*	Yes	Yes
Country *b*	Yes	Yes
Month	Yes	Yes
Fit statistics		
Observations	1,753,290	1,753,290
R^2	0.46878	0.47417
Within R^2	0.19964	0.20776

Clustered (pair) standard-errors in parentheses
*Signif. Codes: ***: 0.01, **: 0.05, *: 0.1*

imbalances results in greater risks. This is the interdependence-contagion hypothesis cited in the policy community - that weak states are risks for their digital neighbors as cyber criminals use gaps in capacity to find safe harbor. Model 2 in Table 4 interacts the level of interconnection with the difference in government effectiveness for dyads.

The interaction term between internet infrastructure interdependence and differences in capacity is negative, indicating that greater gaps in capacity are associated with a weaker effect of interdependence on shared digital threats. Each one unit increase in the relative capacity between two states is associated with a 0.191 decrease in the effect of interdependence on shared threat. For two states with equal levels of capacity like the United States and

Japan, a 1% increase in internet interdependence is associated with a .98% increase in shared digital threats. However, for dyads with a 1 unit difference in capacity like the United States and Uruguay, a 1% increase in internet interdependence is associated with a .78% increase in shared digital threats.

Why does the association between interdependence and shared threat vary with differences in capacity? Interdependence is highly associated with negative digital security externalities, but states and internet service providers are also aware of this. While malicious programs have the potential to exploit differences in capacity, greater differences in capacity also provide more powerful states with the ability to shape the politics in less powerful states and create cooperation regimes. A key feature of the main dependent variable - internet interconnection - helps explain why interdependence is a weaker predictor of shared digital threats as gaps in capacity increase.

7 Asymmetric Dependence and Digital Regimes

The first twenty years of cybersecurity cooperation was marked by a lack of global institutional arrangements to coordinate policy responses (Craig and Valeriano, 2018). Despite gaps at the global level, there has been significant cooperation on cybersecurity at the bilateral and regional level. This includes the European Union Agency for Cybersecurity (2004), the Cybersecurity Program of the OAS Inter-American Committee against Terrorism (2008), the Middle East Regional Cybersecurity Centre sponsored by Oman and the ITU (2013), and the ASEAN-Japan Cybersecurity Capacity Building Centre (2018). As many authors have argued, regional orders work alongside international orders, and may have their own hierarchies that manifest in regional regimes (Buzan and Wæver, 2003). There are reasons to expect that the internet will work this way - at the technical level it is organized by regional internet registries and is characterized by significant preferential attachment.

Australia in the South Pacific helps demonstrate the logic of this paper's empirical findings. The model in the paper predicts that malicious programs that victimize Australian computers, or which use Australian computers to harm others, are more likely to also use servers in countries, or victimize users in countries, where Australia is more digitally interdependent. At the same time, Austrlia exchanges data with many countries, and has varying degrees of interdependence with those countries. This threat environment may also be influenced by the capacity of those states that are interdependent with Australia. Ten agreements between Australia and New Zealand (a high cybersecurity capacity state) may lead to less shared digital threat than ten agreements between Australia and Papua New Guinea (a low cybersecurity capacity state).

However, the model in this paper demonstrates that the opposite is true. For states like Australia, greater interdependence with a state that has high capacity leads to more shared threat than greater interdependence with a state that has low capacity. One explanation for this may be an intervening step - greater gaps in capacity lead to greater adjustment on the part of less powerful states. This would be to asymmetric dependence - if the two countries were to reduce their interdependence the less capable would suffer significantly more. The technical characteristics of the internet support this model of influence.

In December 2020, the final month of the internet measurements in this paper, Australian internet service providers maintained provider-to-customer interconnection agreements with 1058 internet service providers in 47 different countries (in addition to many agreements between providers within Australia). The model in this paper predicts that this should mean Australia faces significantly more shared digital threats with these 47 IP spaces than any of the other 202 IP spaces on the internet. When the manager of one of those 47 IP spaces (the cybersecurity or internet authority in a country) shuts down malicious servers in their space, they disrupt the same threat networks that create risk for Australia. Many of these agreements are with high-capacity countries, including the the United States (572 agreements), New Zealand (429 agreements), and Great Britain (52 agreements). However, data also flows between through agreements between Australia and Vanuatu (8 agreements), Fiji (7 agreements), and Papua New Guinea (7 agreements). Each additional agreement between Australia and Vanuatu contributes to shared threat less than each additional agreement between Australia and Great Britain.

When states are dependent on others, or lack substitutes for important goods, they should be the most likely to accept conditions on future policies and behaviors (Hirschman, 1945; Keohane and Nye, 1973). The source of this power on the internet is partially due to the nature of the internet system - a feature called preferential attachment. Preferential attachment is a feature of some networks where new nodes prefer to make connections with more connected existing nodes (Barabási and Albert, 1999; Krapivsky, Redner and Leyvraz, 2000; Merton, 1968). This is because more connected existing nodes are more valuable for new nodes. For example, a new internet service provider would want to make a connection with a larger provider to benefit from their access to more systems. Several authors have demonstrated that autonomous systems display this behavior (Chang, Jamin and Willinger, 2006; Chen et al., 2002; Subramanian et al., 2002).[31]

Shared threat may help us understand why states cooperate in cyberspace, and the relationship between differences in capacity and shared threat may help understand when this cooperation most successful and deepest. Fischer (1988) lays out four forms of cooperation - exchanging information, negotiating one-off policy deals, creating rules guiding policy choice, and delegating national policy instruments to form an international community. These may take the form of an international regime, where "Implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations" (Krasner, 1982). However, in highly asymmetric relationships we should not expect the more powerful state to delegate its national policy to an international community, but instead exert its influence to capture national policy instruments from less

[31] While the Barabasi-Albert model (1999) of internet development has been much debated, the basic assumption that internet networks have some degree of preferential attachment is settled. The remaining debate surrounds how distribution and strength of this effect. Farrell and Newman (2019) cite Barabási and Albert (1999) as part of their mechanism for weaponized interdependence, but their mechanism is distinct from the one in this paper. For Farrell and Newman (2019), power comes from the ability to cut states out of the system or observe their actions, and the United States is the main example of such a state. In this paper the process is occurring at the regional level, and the mechanism is a more traditional form of dependency.

powerful states.

Australia's cooperation regime in the South Pacific goes beyond sharing best practices or negotiating one-off policy deals - it has supported regional cybersecurity regime that shaped the domestic institutions designed to implement policy. The motivation for this strategy was articulated in Australia's first cybersecurity strategy, published in 2009, that "given the transnational nature of the Internet, in which effective cyber security requires coordinated global action, Australia must adopt an active, multi-layered approach to international engagement on cyber security."[32] The strategy outlines how computer emergency response teams will coordinate international cooperation, engagement in regional and global policy initiatives, and develop best practices. Australia's 2016 strategy also recognizes the risks of gaps in capacity and incentives for capacity building in the region.

> Most cybercrime targeting Australians originates overseas, so the Government will partner with international law enforcement, intelligence agencies and other computer emergency response teams. This will build cyber capacity to prevent and shut down safe havens for cyber criminals. Australia's capacity building assistance will also enable our international partners, particularly in the Indo-Pacific region, to develop their institutional capacity to tackle cyber security threats.[33]

If most cybercrime in Australia originates overseas, the analysis in this paper demonstrates that those overseas locations will be where Australia is most interdependent. The South Pacific's path to the international internet ecosystem has been through the Southern Cross Cable. This 28,900KM cable connects Silicon Valley and Seattle with Australia via Hawaii, New Zealand, and Fiji. It cost approximately $1.5B USD when it was completed in 2000 and has been upgraded multiple times to keep up with increased bandwidth demand.[34] This

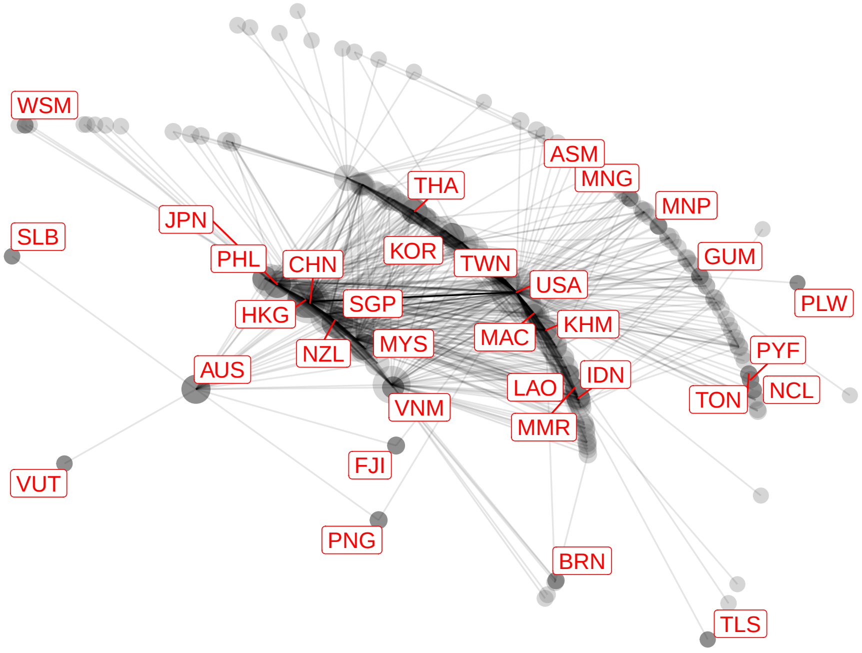
[32] Commonwealth of Australia. "Cyber Security Strategy," 2009. Page VII.

[33] Commonwealth of Australia. "Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity," April 21, 2016. p. 7.

[34] Submarine Cable Networks. "Southern Cross Cable System Overview," May 31, 2011.

physical infrastructure is reflected in the internet interconnection patterns in the region. Figure 3 presents the internet interconnection network in the South Pacific - internet traffic between this region with the global architecture passes through Australian systems. The network is the average number of connections between each node between July 2015 and December 2020. The dense nature of the network makes it difficult to visualize. For this reason, I trim the network using the disparity filter algorithm to identify the backbone structure of the weighted network (Serrano, Boguñá and Vespignani, 2009). The network is plotted using the GGRAPH package in ℝ with the focus mapping method presenting Vanuatu's view of the overall network (Brandes and Pich, 2010).

Figure 3: South-Pacific-Focused Interconnection Network



This figure shows the internet provider-to-customer network for 2020, where edges are the monthly average number of interconnection agreements between internet service providers in the two countries. The network is then trimmed using the backbone algorithm (Serrano, Boguñá and Vespignani, 2009), and plotted with `igraph` using the "focus" method (Brandes and Pich, 2010) on Vanuatu.

The preferential attachment discussed by Chang, Jamin and Willinger (2006); Chen et al.

https://www.submarinenetworks.com/en/systems/trans-pacific/southern-cross/southern-cross-cable-system-overview.

(2002); Subramanian et al. (2002) is reflected in Figure 3. Internet service providers in the South Pacific rely nearly exclusively on interconnection agreements with Australian service providers, including in Fiji (7 of 16 agreements), Vanuatu (8 of 11 agreements), Papa New Guinnea (7 of 16 agreements), and the Solomon Islands (3 of 7 agreements). Australia can credibly increase the barriers to internet access for less-capable states in the South Pacific in ways that it cannot for more capable states in the same region or less-capable states in other regions. New Zealand has an internet interconnection ecosystem that makes it interdependent with Australia (111 of 208 agreements), which indicates that the two states face significant shared threats. However, New Zealand's position within the network is such that it does not depend on Australia as heavily as Fiji, because internet service providers maintain interconnection agreements with providers in 16 countries including the United States (61 of 208).

While this position creates network power, Australia has incentives to promote cooperation because the internet architecture in the South Pacific presents potential risks. One of the risks is that threats will use the internet space in the South Pacific to target more dynamic threats at Ausralian internet users, another is the risks of second-order interdependence. Fear of second-order interdependence came to a head when the Solomon Islands and Papua New Guinea planned to work with Chinese firm Huawei to build a cable between the two islands and Australia.[35] Huawei's products were under increasing scrutiny from regulators regarding their security and protection from spying. In 2018, Australia agreed to pay $92.5M to fund the Coral Sea Cable after pressuring the Solomon Islands and Papua New Guinea to cancel a contract with the Huawei.[36] In Figure 3 we see that the only meaningful interconenction agreements that Solomon Islands internet providers have is with providers in Australia, and providers in Papua New Guinea maintains connections with the United States and Australian

[35] Westbrook, Tom. "PNG Upholds Deal with Huawei to Lay Internet Cable, Derides Counter-Offer." *Reuters*, November 26, 2018, sec. Media and Telecoms. https://www.reuters.com/article/us-papua-huawei-tech-idUSKCN1NV0DR.

[36] Cherney, Mike. "No Way, Huawei: Australia Looks to Cut China's Line Into South Pacific." *Wall Street Journal*, April 20, 2018, sec. World. https://www.wsj.com/articles/no-way-huawei-australia-looks-to-cut-chinas-line-into-south-pacific-1524214738.

providers. While interconnection creates new vectors for threat, and new potential risks, the countries in the South Pacific rely on Australia to facilitate their access to the internet ecosystem.

As a result of its interdependence and the risks it generates, Australia established a Cyber Cooperation Program in 2016, and has dedicated over $34m to "champion an open, free and secure Internet that protects national security and promotes international stability, while driving global economic growth and sustainable development."[37] In 2017, Australia became one of the few countries with cybersecurity strategy exclusively focused on international cooperation and partnerships,[38] and Australia has had an Ambassador for Cyber Affairs within the Department of Foreign Affairs and Trade since 2016. Australia's strategy focuses on the country's neighbors, noting that "It is here, in the Indo-Pacific, that Australia can best leverage our cyber capacity building resources to support and open, free and secure Internet."[39] The analysis in this paper demonstrates that this is not only the region where Australia might be most likely to influence others, it is also the region where interconnection opens the Australia to the potential for shared threat.

Australia's cooperation regime successfully shaped the institutions of its South Pacific neighbors - Samoa, Tonga, Vanuatu, and the Solomon Islands - over the past ten years. The most extreme version of this has occurred over the past decade in Vanuatu. In 2011, only 9.2% of individuals in Vanuatu used the internet, it had one of the world's least developed ICT infrastructures, and among the lowest levels of ICT skills proficiency.[40] In 2008 Vanuatu created the Telecommunications Radiocommunications and Broadcasting Regulator (TRBR) to implement a new set of internet regulations. That year Vanuatu

[37] Australia's International Cyber and Critical Tech Engagement. "Cyber and Critical Tech Cooperation Program." Accessed September 2, 2021. https://www.internationalcybertech.gov.au/cyber-tech-cooperation-program.

[38] The others are China (2013), Japan (2013), the Netherlands (2017), Norway (2017), and the United States (2011).

[39] Commonwealth of Australia. "Australia's International Cyber Engagement Strategy." Department of Foreign Affairs and Trade, October 2017. Page 6.

[40] International Telecommunications Union. "World Telecommunication/ICT Indicators Database." Database, July 2021. https://www.itu.int:443/en/ITU-D/Statistics/Pages/publications/wtid.aspx.

reported to the ITU that it received 100% of the funding for its national telecommunications regulator from an Australian through the World Bank designed to support a the shift from a telecommunications monopoly to a fully liberalised telecommunications sector.[41] In 2011 the national review of aid effectiveness in Australia recommended building on the success of technical assistance programs, and "Review Panel members have seen the impact high–quality specialist advice can have, for example in telecommunications in Vanuatu and in the reform of government financial management in Indonesia."[42]

Vanuatu later delegated cybersecurity policy to the Office of the Government Chief Information Officer (OGCIO), which received funds for technical advisors from Australia.[43] In 2013, the OGCIO developed, and Vanuatu published, an seventy-two-page ICT strategy and a cybersecurity strategy which discuss multi-stakeholder and multi-sector collaboration, private sector development, governance, and "being a responsible member of the international and regional community." Vanuatu cybersecurity advisor Jeff Garae to the program summed it up well when he stated "In the Pacific, just because an economy is small population-wise, it doesn't mean your problem's different from a developed nation — we're accessing the same Internet."[44] The national cybersecurity strategy was published the same year. Vanuatu Prime Minister Moana Carcasses Katokai Kolasil's introduction to the strategy states the motivation was "the arrival of the Interchange Submarine Cable project will provide a high-speed reliable link for Vanuatu to the World. This means internet users at large are exposed to risks experienced by other countries."[45]

Soon after publishing its policy in 2013, Vanuatu completed a $32M project to deploy its first international submarine cable system, joining the Southern Cross cable between

[41] "Vanuatu Telecommunications & ICT Technical Assistance Program." The World Bank, June 30, 2013. https://documents1.worldbank.org/curated/en/190611468121735604/text/934050BRI00PUB0tu0Box385381B0090610.txt.

[42] Holloway, Sandy, Bill Farmer, Margaret Reid, John Denton, and Stephen Howes. "Independent Review of Aid Effectiveness." Australian Government, April 2011.

[43] Samuel, Fred. "Annual Report." Vanuatu: Office of the Government CIO, 2014. https://ogcio.gov.vu/images/Docs/annual_reports/2014_OGCIO_Annual_Report_FINAL.pdf.

[44] McFillin, Adam. "The Road to a National CERT in Vanuatu." APNIC Blog (blog), April 23, 2019. https://blog.apnic.net/2019/04/23/the-road-to-a-national-cert-in-vanuatu/.

[45] Government of Vanuatu. "National Cybersecurity Policy," December 2013. P. 3.

Sydney and the United States. Within three years of publishing its policies and operating this cable, fixed-broadband basket prices went from $86.51 (PPP) to $50.96 (PPP) as world prices stayed flat and prices in developing countries went down only $6.10 (PPP). Google assisted by setting up a cache server to support a new IXP, directly facilitating the type of interconnection featured in this paper's empirical analysis.[46] However, cooperation between Australia and Vanuatu continued after the telecommunications infrastructure was in place.

Vanuatu's Computer Emergency Response Team (CERT-VU), responsible for carrying out Vanuatu's cybersecurity strategy, signed a Memorandum of Understanding with the Australian government as part of a bilateral security treaty in 2018. This treaty also came with AUD 400,000 in aid to strengthen Vanuatu's cybersecurity capabilities.[47] This is one case in a larger trend in the region. Australia provided technical assistance to the Ministry of Communications and Information Technology of Samoa to align legislation with the Budapest Convention on Cybercrime and funded the National Cyber Security Center of Papua New Guinea,[48] which later commissioned and published a report on cybersecurity practices at a Huawei data center that disrupted Chinese digital investment in the country. Australia institutionalized regional cooperation program in 2018 through the Pacific Cyber Security Operational Network (PaCSON). Several of the institutions participating in PaCSON were either founded by or received funding from the Australian government.

The South Pacific may help us understand why differences in state capacity are negatively associated with the effect of interdependence on shared threat. Distance between countries reduces negative externalities when accounting for interconnection, where one plausible hypothesis is that lesser distance increases cooperation. Here, I show how a regional power, which is exposed to negative externalities from neighbors with lower levels of state capacity, successfully invested in bilateral assistance and regional cooperation. When gaps between

[46] An IXP, or internet exchange point, is a physical location where different internet service providers can exchange data across their networks. By agreeing to exchange data at an IXP, these providers can reduce their reliance on upstream transit and thus reduce their costs.

[47] McFillin, Adam. "The Road to a National CERT in Vanuatu." APNIC Blog (blog), April 23, 2019. https://blog.apnic.net/2019/04/23/the-road-to-a-national-cert-in-vanuatu/.

[48] https://png.embassy.gov.au/pmsb/784.html

interdependent states are greater certain forms of cooperation may become more likely, including capacity building, information sharing, and technical assistance that harmonizes standards and policies across countries.

8 Conclusion

The internet presents a challenge for states managing globalization - it is both a highly interdependent and open system. Transnational crime and cybersecurity threat networks operate across national borders, and internet users in states with the lowest capacity use the same global network as those in states with the highest capacity. This paper investigates how digital interdependence - as measured by the integration between networks in two countries - translates into shared digital threats - as measured by the number of digital threats leveraging hosts in two countries.

I theorize that the internet's structure is an essential form of interdependence for shared digital threats since malicious programmers try to be near potential victims and limit their geographic scope. For delivering threats to any given country, the most attractive location to host attacks should be in adjacent IP spaces that are heavily integrated. The analysis confirmed this model of shared threat - interdependence at the internet level explains co-hosted digital threats independently of geography or trade flows.

The open nature of the internet motivates widespread fear among the international community. International organizations, the business community, and governments fear that low-capacity states integrated with high-capacity states will become safe havens for malicious online activity. At the same time, these communities believe that transnational cooperation will lessen the impact of interdependence on shared threats, and high-capacity states may be in a better position to compel their lower-capacity partners to share information and coordinate cybersecurity response. Countering the narrative of contagion from weak states online, this paper's analysis demonstrates that interdependence's effects on shared threat is the largest when capacity gaps are small.

I theorize that the lack of contagion is due to cooperation between high and low capacity states enabled by preferential attachment on the internet. When new internet service providers enter the internet architecture they seek partners that can easily facilitate their access to the global system. These new providers are most likely to be in developing states, while existing nodes with a wide reach are most likely to be in developed states. In the South Pacific, states such as Vanuatu, Papua New Guinea, and Fiji rely heavily on connections with providers in Australia, which has invested heavily in a cooperative regime to build trust and threat sharing networks in the region. These power imbalances encourage deep forms of cooperation that would be unlikely among equally powerful states.

There are several other areas for future work. Since the internet is a global network, cybersecurity presents a series of coordination and cooperation challenges, many of which have not been addressed in this paper. Nadji et al. (2013) demonstrate that disabling 20% of a criminal network's hosts reduces the overall success of the criminal network's hosting by 70%. The entire network becomes degraded if one part of it is disrupted. This analysis suggests that the states who are most likely to benefit if one country shuts down hosts are those they are most interdependent with. If one country's investment in security presents positive externalities for other countries there may be incentives to free-ride, conflict over who should pay for security, or pressure to create institutions to lessen a cooperation dilemma. The focus in this paper was whether interdependence is at the core of why these networks span states, and whether gaps in capacity contribute to shared risk. However, other conflict and cooperation may emerge as states try to limit the expected $6 trillion yearly losses due to digital threats.

There may also be different forms of cooperation that may emerge from increasing interdependence. This paper suggests that capacity building is one area, but there are many different forms of potential digital security cooperation, or cases when we might expect multilateral responses. For instance, countries that co-host malware with many different countries may prefer multilateral responses through institutions such as the International

Telecommunications Union, while countries hosting programs with few countries may prefer bilateral cooperation. There may also be different domains of cooperation that are driven by these agreements - for instance, they may result in greater cooperation on technical measures, but not joint efforts on norms. They may promote cooperation between different parts of government, such as bilateral cooperation between CERTS. This paper has provided a first look at how the internet has created shared threats and insights into how states can exert power within networks, and contributes to the literature on globalization, cooperation, transnational networks, and technology.

Another area for future research is whether shared digital risk causes countries to reduce their interdependence. If interconnection creates shared threats to internet users, the digital divide may be driven by a failure of countries to convince potential partners that they can effectively manage cyberspace. Measures that promote cooperation may then promote integration among internet service providers. One question is why states do not exert greater control over data flows given the fact that they lead to particular security challenges. This analysis suggests that these decisions made by independent operators results in greater threat, but why they continue to open up data flows is another matter. Decoupling has become a larger part of the policy debate after the Justice Department decision in 2019 to block a submarine internet cable from Los Angeles to Hong Kong. It is possible that the economic benefits of these agreements outweigh the costs of increased security challenges for governments, or that private firms lobby governments to limit regulation. It may be that this negative externality is priced in at the interconnection level - that the price of internet interconnection rates is higher from countries with lax cybersecurity.

References

Anderson, James E. 2011. "The Gravity Model." *Annual Review of Economics* 3(1):133–160.

Antonakakis, Manos, Roberto Perdisci, David Dagon, Wenke Lee and Nick Feamster. 2010. Building a Dynamic Reputation System for DNS. In *Proceedings of the 19th USENIX Conference on Security.* USENIX Security'10 USA: USENIX Association p. 18.

Antonakakis, Manos, Roberto Perdisci, Wenke Lee, Nikolaos Vasiloglou and David Dagon. 2011. Detecting Malware Domains at the Upper DNS Hierarchy. In *Proceedings of the 20th USENIX Conference on Security.* SEC'11 USA: USENIX Association p. 27.

Atzili, Boaz. 2007. "When Good Fences Make Bad Neighbors: Fixed Borders, State Weakness, and International Conflict." *International Security* 31(3):139–173.

Baldwin, David A. 1985. *Economic Statecraft.* Princeton, N.J: Princeton University Press.

Baldwin, Richard and Daria Taglioni. 2006. Gravity for Dummies and Dummies for Gravity Equations. Technical Report w12516 National Bureau of Economic Research Cambridge, MA: .

Barabási, Albert-László and Réka Albert. 1999. "Emergence of Scaling in Random Networks." *Science* 286(5439):509–512.

Beardsley, Kyle. 2011. "Peacekeeping and the Contagion of Armed Conflict." *The Journal of Politics* 73(4):1051–1064.

Bellasio, Jacopo, Richard Flint, Nathan Ryan, Susanne Sondergaard, Cristina Gonzalez Monsalve, Arya Sofia Meranto and Anna Knack. 2018. Developing Cybersecurity Capacity: A Proof-of-Concept Implementation Guide. Technical report Rand Corporation.

Bilge, Leyla, Sevil Sen, Davide Balzarotti, Engin Kirda and Christopher Kruegel. 2014. "Exposure: A Passive DNS Analysis Service to Detect and Report Malicious Domains." *ACM Transactions on Information and System Security* 16(4):1–28.

Brandes, Ulrik and Christian Pich. 2010. More Flexible Radial Layout. In *Graph Drawing*, ed. David Eppstein and Emden R. Gansner. Lecture Notes in Computer Science Berlin, Heidelberg: Springer pp. 107–118.

Brooks, Stephen G. and William Curti Wohlforth. 2008. *World out of Balance: International Relations and the Challenge of American Primacy.* Princeton: Princeton University Press.

Buhaug, Halvard and Kristian Skrede Gleditsch. 2008. "Contagion or Confusion? Why Conflicts Cluster in Space1." *International Studies Quarterly* 52(2):215–233.

Buzan, Barry and Ole Wæver. 2003. *Regions and Powers: The Structure of International Security.* Number 91 *in* "Cambridge Studies in International Relations" Cambridge ; New York: Cambridge University Press.

Carter, David B. and Paul Poast. 2020. "Barriers to Trade: How Border Walls Affect Trade Relations." *International Organization* 74(1):165–185.

Chang, H., S. Jamin and W. Willinger. 2006. To Peer or Not to Peer: Modeling the Evolution of the Internet's AS-Level Topology. In *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications.* pp. 1–12.

Chen, Qian, Hyunseok Chang, R. Govindan and S. Jamin. 2002. The Origin of Power Laws in Internet Topologies Revisited. In *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies.* Vol. 2 pp. 608–617 vol.2.

Cheung, William, Scott Fung and Shih-Chuan Tsai. 2010. "Global Capital Market Interdependence and Spillover Effect of Credit Risk: Evidence from the 2007–2009 Global Financial Crisis." *Applied Financial Economics* 20(1-2):85–103.

Clegg, Richard G., Carla Di Cairano-Gilfedder and Shi Zhou. 2010. "A Critical Look at Power Law Modelling of the Internet." *Computer Communications* 33(3):259–268.

Clemente, Dave and Royal Institute of International Affairs. 2013. *Cyber Security and Global Interdependence: What Is Critical?* London: Chatham House, The Royal Institute of International Affairs.

Coe, David T. and Elhanan Helpman. 1995. "International R&D Spillovers." *European Economic Review* 39(5):859–887.

Conley, Timothy G. and Giorgio Topa. 2002. "Socio-Economic Distance and Spatial Patterns in Unemployment." *Journal of Applied Econometrics* 17(4):303–327.

Cooper, Richard N. 1986. *Economic Policy in an Interdependent World: Essays in World Economics.* Cambridge, Mass: MIT Press.

Corsetti, Giancarlo, Marcello Pericoli and Massimo Sbracia. 2005. "'Some Contagion, Some Interdependence': More Pitfalls in Tests of Financial Contagion." *Journal of International Money and Finance* 24(8):1177–1199.

Craig, Anthony and Brandon Valeriano. 2018. "Realism and Cyber Conflict: Security in the Digital Age.".

Davis, Lance E., Douglass C. North and Calla Smorodin. 1971. *Institutional Change and American Economic Growth.* Cambridge [Eng.]: University Press.

Dhamdhere, Amogh and Constantine Dovrolis. 2010. The Internet Is Flat: Modeling the Transition from a Transit Hierarchy to a Peering Mesh. In *Proceedings of the 6th International COnference.* Co-NEXT '10 New York, NY, USA: Association for Computing Machinery pp. 1–12.

Diehl, Paul F, Gary Goertz and Yahve Gallegos. 2019. "Peace Data: Concept, Measurement, Patterns, and Research Agenda." *Conflict Management and Peace Science* p. 073889421987028.

D'Ignazio, Alessio and Emanuele Giovannetti. 2009. "Asymmetry and Discrimination in Internet Peering: Evidence from the LINX." *International Journal of Industrial Organization* 27(3):441–448.

Drezner, Daniel W. 2003. "The Hidden Hand of Economic Coercion." *International Organization* 57(3):643–659.

Drezner, Daniel W. 2008. *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton: Princeton Univ. Press.

Drezner, Daniel W. 2015. "Targeted Sanctions in a World of Global Finance." *International Interactions* 41(4):755–764.

EastWest Institute. 2012. Building Trust in Cyberspace. In *3rd Worldwide Cybersecurity Summit*. New Delhi: .

Erlander, Sven and Neil F. Stewart. 1990. *The Gravity Model in Transportation Analysis: Theory and Extensions*. VSP.

Ertur, Cem and Wilfried Koch. 2006. Convergence, Human Capital and International Spillovers. Technical Report 2006-03 LEG, Laboratoire d'Economie et de Gestion, CNRS, Université de Bourgogne.

Executive Office of the President. 2017. "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.".

Farrell, Henry and Abraham Newman. 2019. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44(1):42–79.

Feaver, Peter and Eric Lorber. 2010. "Coercive Diplomacy and the New Financial Levers: Evaluating the Intended and Unintended Consequences of Financial Sanctions." *SSRN Electronic Journal* .

Findlay, Mark. 2000. *The Globalisation of Crime Understanding Transitional Relationships in Context*. Cambridge: Cambridge University Press.

Fischer, Stanley. 1988. Macroeconomic Policy Coordination. In *Internaitonal Economic Cooperation*, ed. Martin Feldstein. Chicago: University of Chicago Press.

Garg, Vaibhav. 2012. "Macroeconomic Analysis of Malware." *SSRN Electronic Journal* .

[Georgia Tech]. N.d. "GT Malware Passive DNS Data Daily Feed.".

Gilpin, Robert and Jean M. Gilpin. 1987. *The Political Economy of International Relations*. Princeton, N.J: Princeton University Press.

Giotsas, Vasileios, Shi Zhou, Matthew Luckie and kc claffy. 2013. Inferring Multilateral Peering. In *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*. Santa Barbara California USA: ACM pp. 247–258.

Gowa, Joanne. 1989. "Bipolarity, Multipolarity, and Free Trade." *The American Political Science Review* 83(4):1245–1256.

Gowa, Joanne. 1994. *Allies, Adversaries, and International Trade.* Princeton, NJ: Princeton Univ. Press.

Gurevich, Tamara and Peter Herman. 2018. "The Dynamic Gravity Dataset: Technical Documentation.".

High-level Panel on Digital Cooperation. 2019. The Age of Digital Interdependence. Technical report United Nations.

Hirschman, Albert O. 1945. *National Power and the Structure of Foreign Trade.* Berkeley :: University of California Press.

Ikenberry, Karl. 2015. "A Grand Strategy for Failed States.".

Karemera, David, Victor Iwuagwu Oguledo and Bobby Davis. 2000. "A Gravity Model Analysis of International Migration to North America." *Applied Economics* 32(13):1745–1755.

Kaufmann, Daniel, Aart Kraay and Massimo Mastruzzi. 2010. The Worldwide Governance Indicators: Methodology and Analytical Issues. Technical Report 5430 The World Bank.

Keller, Wolfgang. 2002. "Geographic Localization of International Technology Diffusion." *American Economic Review* 92(1):120–142.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy.* 1st princeton classic ed ed. Princeton, N.J: Princeton University Press.

Keohane, Robert O. and Joseph S. Nye. 1973. "Power and Interdependence." *Survival* 15(4):158–165.

Kindleberger, Charles Poor. 1973. *The World in Depression, 1929-1939: 40th Anniversary of a Classic in Economic History.* Berkeley: University of California Press.

Krapivsky, P. L., S. Redner and F. Leyvraz. 2000. "Connectivity of Growing Random Networks." *Physical Review Letters* 85(21):4629–4632.

Krasner, Stephen D. 1982. "Structural Causes and Regime Consequences: Regimes as Intervening Variables." *International Organization* 36(2):185–205.

Lake, David A. 2009. *Hierarchy in International Relations.* Cornell Studies in Political Economy Ithaca, NY.: Cornell Univ. Press.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace.* New York: Basic Books.

Lopez Gonzalez, Javier and Janos Ferencz. 2018. Digital Trade and Market Openness. OECD Trade Policy Papers 217.

Merton, Robert K. 1968. “The Matthew Effect in Science.” *Science* 159(3819).

Metternich, Nils W., Shahryar Minhas and Michael D. Ward. 2017. “Firewall? Or Wall on Fire? A Unified Framework of Conflict Contagion and the Role of Ethnic Exclusion.” *Journal of Conflict Resolution* 61(6):1151–1173.

Mezzour, Ghita L., L. Richard Carley and Kathleen M. Carley. 2014. Global Mapping of Cyber Attacks. Technical Report CMU-ISR-14-111 Carnegie Mellon University Pittsburgh, PA 15213: .

Milner, Helen V. 1997. *Interests, Institutions, and Information: Domestic Politics and International Relations*. Princeton, N.J: Princeton University Press.

Moreno, Ramon and Bharat Trehan. 1997. “Location and the Growth of Nations.” *Journal of Economic Growth* 2(4):399–418.

Nadji, Yacin, Manos Antonakakis, Roberto Perdisci and Wenke Lee. 2013. Connected Colors: Unveiling the Structure of Criminal Networks. In *Research in Attacks, Intrusions, and Defenses*, ed. Salvatore J. Stolfo, Angelos Stavrou and Charles V. Wright. Lecture Notes in Computer Science Berlin, Heidelberg: Springer pp. 390–410.

Naylor, R. T. 2004. *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*. Rev. ed ed. Ithaca: Cornell University Press.

Nye, Joseph. 2016. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41(3):44–71.

Oneal, John R., Frances H. Oneal, Zeev Maoz and Bruce Russett. 1996. “The Liberal Peace: Interdependence, Democracy, and International Conflict, 1950-85.” *Journal of Peace Research* 33(1):11–28.

Patrick, Stewart. 2007. “”Failed” States and Global Security: Empirical Questions and Policy Dilemmas.” *International Studies Review* 9(4):644–662.

Perdisci, Roberto, Igino Corona, David Dagon and Wenke Lee. 2009. Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces. In *2009 Annual Computer Security Applications Conference*. pp. 311–320.

Perdisci, Roberto, Wenke Lee and Nick Feamster. 2010. Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces. In *Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation*. NSDI’10 USA: USENIX Association p. 26.

Pollins, Brian M. 1989. “Does Trade Still Follow the Flag?” *American Political Science Review* 83(2):465–480.

Rahbarinia, Babak, Roberto Perdisci and Manos Antonakakis. 2016. “Efficient and Accurate Behavior-Based Tracking of Malware-Control Domains in Large ISP Networks.” *ACM Trans. Priv. Secur.* 19(2).

Rieck, Konrad, Thorsten Holz, Carsten Willems, Patrick Düssel and Pavel Laskov. 2008. Learning and Classification of Malware Behavior. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, ed. Diego Zamboni. Lecture Notes in Computer Science Berlin, Heidelberg: Springer pp. 108–125.

Salehyan, Idean and Kristian Skrede Gleditsch. 2006. "Refugees and the Spread of Civil War." *International Organization* 60(2):335–366.

Schönenberg, Regine and Annette von Schönfeld. 2013. Introduction. In *Transnational Organized Crime*, ed. Regine Schönenberg and Heinrich-Böll-Stiftung. Analyses of a Global Challenge to Democracy Transcript Verlag pp. 11–16.

Serrano, M. Ángeles, Marián Boguñá and Alessandro Vespignani. 2009. "Extracting the Multiscale Backbone of Complex Weighted Networks." *Proceedings of the National Academy of Sciences* 106(16):6483–6488.

Shelley, Louise. 1995. "Transnational Organized Crime: An Imminent Threat to the Nation-State?" *Journal of International Affairs* 48(2).

Simmons, Beth A., Paulette Lloyd and Brandon M. Stewart. 2018. "The Global Diffusion of Law: Transnational Crime and the Case of Human Trafficking." *International Organization* 72(2):249–281.

Subramanian, L., S. Agarwal, J. Rexford and R.H. Katz. 2002. Characterizing the Internet Hierarchy from Multiple Vantage Points. In *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies.* Vol. 2 pp. 618–627 vol.2.

The Council of Economic Advisors. 2018. The Cost of Malicious Cyber Activity to the U.S. Economy. Technical report.

The White House. 2018. "National Cyber Strategy of the United States of America.".

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System.* New York: Oxford University Press.

Williams, Phil and Dimitri Vlassis, eds. 2001. *Combating Transnational Crime: Concepts, Activities, and Responses.* London ; Portland, OR: Frank Cass.

Zhuo, Ran, Bradley Huffaker, KC Claffy and Shane Greenstein. 2021. "The Impact of the General Data Protection Regulation on Internet Interconnection." *Telecommunications Policy* 45(2).

Zignago, Soledad and Thierry Mayer. 2005. Market Access in Global and Regional Trade. Sciences Po Publications 2005-02 Sciences Po.