Does Data Follow the Flag?

Harry Oppenheimer *
Updated: October 20, 2022

For the most current version of this paper please use the Dropbox link
(https://www.dropbox.com/s/pp8ytt9xn9jaqnx/dataflag_101722.pdf?dl=0)

Abstract

Does data follow the flag? Although the internet is central to international economic and security competition, we know little about the geopolitics of data flows. Due to its diffuse structure, the internet is typically described as "un-territorial" and resistant to border effects. Yet, the private firms that negotiate the internet's structure manage economic and security risks. This paper identifies three ways that international conflict may influence data routes - through reductions in non-digital trade, business risks from sanctions and cyberattacks, and increased threat from weaponized interdependence and spying, and tests whether international conflict and security treaties influence how the internet routes data across borders. Despite widespread spying and weaponized interdependence between allies, military treaties are associated with new data pathways. I theorize that this is because spying between allies does not create security externalities, reducing the risk from weaponized interdependence. Surprisingly, international conflict is associated with increases in data pathways. However, Russia-Ukraine conflict since 2014 demonstrates how territorial conquest yields digital control, which can be used to consolidate occupation. Removing this conflict yields a negative relationship between data routes and the remaining international conflicts. This paper demonstrates how international security and risk shape the global digital economy and technical infrastructures.

Word Count: 11,200 (including footnotes and bibliography)

*PhD Candidate, Harvard University. 1737 Cambridge St, Cambridge MA 02138.
Email: hoppenheimer@g.harvard.edu
Website: https://scholar.harvard.edu/hoppenheimer

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

–John Perry Barlow, "A Declaration of the Independence of Cyberspace"

1 Introduction

Does international security shape how data moves across borders? The internet is often describes as an ideal case of a privately run system with networked governance (Mueller, Schmidt and Kuerbis, 2013; van Eeten and Mueller, 2013). A multi-stakeholder non-profit organizes many internet protocols, and individual private firms negotiate data routes. International organizations create globally accepted and implemented security and data practices. Due to its decentralized structure, many observers predicted that the internet would be free from government intervention and regulation, bring the "death of distance," "un-territorial," disrupt traditional sovereignty, and foster a global society with open exchange (Daskal, 2015; Cairncross, 1997; Froomkin, 1997; Johnson and Post, 1996; Kobrin, 2001; Svantesson, 2017; Swire, 1998).

Yet, the open, decentralized, and market-driven vision for the internet frequently confronts the challenges of international politics. For data to move across the world - for networks to network - internet service operators in different countries and regulatory environments must agree to transit data. Lessig (1999) argued that the internet's technical structure constrains individuals' behaviors, and authors argue that *domestic* politics can shape internet infrastructure and adoption (Guillén and Suárez, 2005; Milner, 2006; Corrales and Westhoff, 2006). However, we have little insight into how international security influences internet's technical structure. The internet is international, and even perhaps "un-territorial," but does data follow the flag?

Economists and political scientists often ask how bilateral political and military relationships impact trade (Berger et al., 2013; Carter, Wellhausen and Huth, 2019; Davis and Meunier, 2011; Hirschman, 1945; Savage and Deutsch, 1960). In addition to traditional trade models balancing factor endowments and comparative advantage, "trade follows the flag" proposes political and military intervention directly influences trade relationships. That conflict may reduce, and alliances may increase, trade beyond what we would expect given stylized assumptions about how goods should flow across borders (Anderton and Carter, 2001; Gowa and Mansfield, 1993, 2004; Keshk, Pollins

and Reuveny, 2004; Long, 2008; Mansfield and Bronson, 1997; Pollins, 1989*b*,*a*).

Data moves between states like other goods and services, and how data flows around the world has substantial economic and security ramifications. Inefficient internet structures in the developing world have led to significant increases in cost and latency, dragging national economies (Chavula et al., 2017; Gupta et al., 2014). Conversely, efficient internet architectures in countries like the Netherlands are a significant economic comparative advantage (Chakravorti and Chaturvedi, 2020). The Snowden leaks demonstrated that how data is routed through the internet enables government-sponsored espionage, an important new source of power through weaponized interdependence (Farrell and Newman, 2019).

This paper identifies three ways that international conflict may influence data routes - through reductions in non-digital trade, business risks for individual firms from sanctions and cyberattacks, and increased threat from weaponized interdependence and spying. Alliances may promote data flows by encouraging non-digital trade, limiting risks to firms negotiating data transit, and reducing security externalities from data flows. Alliances have not prevented states from using digital interdependence to spy on one another. If internet service providers fear spying from foreign governments, alliances may marginally influence data flows. Yet, alliances reduce security externalities, so military alliances may still promote data flows by reducing the *value* of information gleaned through spying and the likelihood that digital spying will be used to gain security advantages.

The paper continues as follows - first, it explains the internet's technical structure, its significance, and the current understanding of how internet operators decide to route data. After, it explains three mechanisms where international conflict could lead to decreases in data flows, and how formal alliances may counteract each of these mechanisms and promote data flows. The paper's empirical test leverages millions of internet topographical measurements and data interconnection agreements between over seventy thousand internet operators between 2006 and 2018.

The analysis shows how military alliances and treaties are positively associated with new data paths between states. Limiting the analysis to countries with existing data infrastructure (fiber-optic cable networks) does not change this result. Perhaps counter-intuitively, large-scale military conflicts are also associated with new data routes between states. However, this result is driven by Russia-Ukraine conflict since 2014, one of the few international conflicts where there was both 1.) high levels of data transit before conflict onset and 2.) annexed territory. I use a case study of Ukrainian internet space after conflict with Russia in 2014 and 2022 to demonstrate how control

over physical territory yields control over the direction of data flows, which in turn can be used to facilitate military occupation. Overall, the paper provides evidence that international security influences a vast decentralized network internet service operators that shape the digital economy.

2 Who Creates the Internet's Structure?

The internet relies on a global concept called the "end-to-end principle" - computers route messages along the network so that two distant nodes can communicate. A set of routing rules, negotiated by each network, determined how information passes through the system. The internet architecture is a series of connected networks that agree to pass packets to one another.

In a national mail system, the government decides how information gets from one place to another - which facilities it moves to, who carries it, how long it will take - the structure of the system. Instead of government top-down control, the internet's structure is created by a community of Autonomous Systems (ASes) - networks or groups of networks controlled by a common administrator. The earliest ASes were universities and institutions from the original ARPANET. The number of systems increased from fewer than 5,000 in 1998 to over 70,000 in 2020.[1] Today, the most common networks are internet service providers, although universities, corporations, and states maintain ASes. Some centralization exists in to facilitate global data transfers. Regional internet registries collect and disseminate information about each network. The first of these, the Réseaux IP Européens Network Coordination, was founded in 1992 in Amsterdam, and during the 1990s other internet registries emerged to coordinate internet exchange in each region. Each registry runs as non-profit, membership-based organizations of providers. Routing rules, however, are negotiated by individual network operators.

For a network to communicate with the larger internet, it can either exchange data directly with other networks or find another network to carry their data. These "peer-to-peer" and "customer-to-provider" agreements carry data between physical locations in digital space. When networks peer they agree to exchange data without charging fees, when they interconnect as customer-to-provider one network agrees to carry data for another for a fee. Typically networks will peer when they are similar sizes and expect symmetric data flows, and agree to carry data when one network depends heavily on another. These information flows both facilitate other commercial activity and are a

[1] Bates, Tony, Philip Smith, and Geoff Huston. "CIDR Report." Accessed March 9, 2022. https://www.cidr-report.org/as2.0/.

commercial activity themselves.

The existing political science literature focuses on how politics shape platforms and applications such as social or mass media. This includes literature on internet filtering and control, how authoritarian regimes censor information, and how politicians mobilize online. Less of this work examines how politics shapes the internet's structure. Several authors examine how politics influence internet development and shapes the digital divide (Henisz and Zelner, 2001; Guillén and Suárez, 2005; Milner, 2006; O'Hara and Hall, 2021). In these cases, the internet is a domestic phenomenon - states can shape or promote its development within their borders. However, a significant portion of data flows are international - networks in different countries agreeing to route data across borders.

Science and technology studies (STS) places greater emphasis on how international factors influence global infrastructures. Technology transfers allowed states to exert imperialist control over developing countries (Headrick, 1988), or international telegraph and telephone cables facilitated empire (Winseck and Pike, 2007) and reflected great power politics (Hills, 2002). DeNardis (2012, 2014) argues that the internet architecture is an arrangement of power - technical control is used to shape how individuals interact with the global system. At the same time, international security may shape how the internet's technical protocols route data worldwide.

3 Why Does Internet Structure Matter?

How internet service providers agree to exchange data - the structure of the internet - significantly influences the speed, price, and reliability of internet access, and security competition. As a result, the structure impacts global inequality (van Dijk and Hacker, 2003) and economic growth (Czernich, Falck, Kretschmer and Woessmann, 2011; Roller and Waverman, 2001). Network science investigates interconnection development, while an adjacent literature in economics measures how the quality of internet provision influences welfare and growth. Finally, new globalization research discusses internet structures as a source of power and intelligence.

Data routing decisions can degrade an entire region's internet. Gupta et al. (2014) find that 66.8% of African internet traffic travels out of the continent to reach another point in Africa, causing data to travel through "circuitous paths."Chavula et al. (2017) show that, because internet service providers were not making agreements to exchange data, data often travels faster between Africa and Europe than within Africa.

In addition to increasing internet speed, increasing internet peering (one of the two forms of interconnection in this paper) is associated with lower internet prices (Baake and Wichmann, 1999; McKnight and Bailey, 1998). Greater interconnection (paid or unpaid) improves reliability, since more connection reduces the dependence on any one data path which could be disrupted due to single faults.[2] Both internet speed and pricing are cited as significant barriers to economic advancement in the developing world.[3]

Developed states discuss their position internet's infrastructure as a comparative advantage. The Netherlands markets itself as the "Digital Gateway to Europe," building the "1000 years the Netherlands has been the (digital) gateway to the European market."[4] A central part of its advantage is the Amsterdam Internet Exchange, AMS-IX, a not-for-profit organization founded in the early 1990s by a consortium of internet service providers that is at the center of the global internet. In 2020, 30% of the 950 internet providers exchanging data at AMS-IX were from outside Europe, 49% were from Europe (excl. Netherlands), and 21% were domestic (Grove and de Lange, 2021). A 2020 report found that the digital infrastructure in the Netherlands accounted for €460 billion, 60% of GNP, and 3.3 million jobs.[5] The Netherlands robust digital platforms and internet infrastructure also made it the second most prepared country for remote work during the COVID-19 pandemic (Chakravorti and Chaturvedi, 2020). A central position in the internet architecture is a resource in itself - it makes states like the Netherlands a hub for the global digital economy.

While internet structure matters for economic development, it may also provide intelligence advantages over adversaries. A country's reliance on others opens it up to coercion from foreign powers through conditionality, sanction, and changing incentives (Drezner, 2003; Hirschman, 1945), and a state's importance in global networks provides opportunities to shape international rules and regimes (Keohane and Nye, 1977; Slaughter, 2017). Recently, Farrell and Newman (2019) argued that centrality within global networks provides direct coercive advantages through "panopticon" and "chokepoint" effects - the ability to monitor the overall network and exclude specific actors from it. The authors' argue that the internet represents a "panopticon" opportunity for the United States,

[2]Gonyea, Ben. "What Is Internet Peering and Why Is It Beneficial." Digital Realty, March 27, 2014.; Doerr, Christian, Razvan Gavrila, Fernando Kuipers, and Panagiotis Trimintzios. "Good Practices in Resilient Internet Interconnection." Report/Study. ENISA, June 2012.; Garnett, Paul. "Connect2Recover: Building Back Better with Broadband." ITU, March 15, 2021.; Ivanov, Ivo. "Another Five Reasons to Peer." APNIC Blog, September 7, 2021. https://blog.apnic.net/2021/09/07/another-five-reasons-to-peer/.

[3]Schumann, Robert, and Michael Kende. "Lifting Barriers to Internet Development in Africa: Suggestions for Improving Connectivity." Internet Society, May 2013.

[4]Digital Gateway to Europe. "Homepage," 2018. https://www.digitalgateway.eu/.

[5]"The Future of the Digital Economy." Pb7 Research and the METISfiles, 2020.

which can leverage the internet's structure with intelligence capabilities to monitor adversaries.

Finally, the internet's structure is important because it allows states to effectively control and censor information. Russia's data control program - "the System for Operative Investigative Activities" or SORM - monitors the internet through telecommunications partners. The companies that operate autonomous systems in Russia have to install a "black box," or internet monitoring device, on their networks to allow Russian intelligence services to collect traffic.[6] The Russian internet censor Roskomnadzor uses direct access to data flows to block websites critical of the government, owned by foreign companies or media, or found to be spreading "fake news."[7] Data from outside of Russia that transits through Russia can be inspected and filtered through the same techniques. Since the physical path that data takes determines the opportunities to use black box and filtering technologies, countries including Russia and China are exerting greater control over internet routing to facilitate greater control over the internet generally (Sivetc, 2021).

4 How Security Influences Data Flows

There are three reasons why international conflict may influence how networks decide to route data out of their networks. Conflict and competition between states may 1.) reduce trade generally, leading to decreased demand for information, 2.) create business risks through sanctions and potential cyberattacks, which interrupt the firms operating the internet backbone, or 3.) increase the value of intelligence, creating security externalities and risks for data flows. Military alliances reduce the fear of security externalities from economic exchange, enforce trade linkages, and create strategic interdependence.

However, evidence that data follows the flag should be surprising given what we have been led to believe - that in contrast to its predecessors such as the telephone and telegraph, the internet inherently difficult to regulate and extraterritorial. This argument starts at the technical level - because the internet is vast, the data routing rules are self-organizing and highly decentralized (Feamster, Winick and Rexford, 2004; Hall, Anderson, Clayton, Ouzounis and Trimintzios, 2011). The internet was pioneered and sustained into the 1990s by groups of engineers with little concern for international politics (Abbate, 1999), and self-regulation dominated the internet for most of its

[6] Lewis, James Andrew. "Reference Note on Russian Communications Surveillance." CSIS.org, April 18, 2014. https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

[7] Human Rights Watch. "Russia: Growing Internet Isolation, Control, Censorship," June 18, 2020. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

history (Price, Verhulst and Verhulst, 2005).

Cairncross (1997) famously argued that the internet meant the "death of distance" for business and the global economy due to decreased transaction costs. Swire (1998) and Froomkin (1997) argued that the internet empowered private actors over states by facilitating forum shopping. Legal scholars faced a challenge regarding how physical-contextual laws applied to digital spaces - Johnson and Post (1996) argued that traditional law could not govern the internet. Daskal (2015) argued that data was fundamentally "un-territorial" due to "ease and speed with which data travels across borders, the seemingly arbitrary paths it takes, and the physical disconnect between where data is stored and where it is accessed." This is similar to arguments made by Kobrin (2001) in the context of digital commerce. These perspectives suggest that territorially-dependent effects (like conflict between countries), should not impact data transfer.

Additionally, data flows may be unconnected to international conflict due to floor effects - countries at risk of attacking one another may be less likely to transit data between one another, and existing data transit links with rivals may be through dominant firms in the data transit market. As Grinberg (2021) notes, states may not be able to produce a good that they trade with an adversary, and so trade may continue even as conflict breaks out. At the global level, the internet is dominated by a small number of firms that leverage network effects to dominate the data exchange market (Barabási and Albert, 1999; Chang, Jamin and Willinger, 2006; Clegg, Di Cairano-Gilfedder and Zhou, 2010; Subramanian et al., 2002). In this case, there may be limited firms that can move data internationally, so they may continue to transit data after conflict begins even if conventional trade decreases, business risks challenge the market, and weaponized interdependence threatens data.

Through Non-Digital Trade

Interstate commerce is often disrupted by military conflict. Bilateral trade is significantly reduced by conventional wars (Glick and Taylor, 2010; Anderton and Carter, 2001), the fear or expectation of future conflicts (Long, 2008), low level conflict (Keshk, Pollins and Reuveny, 2004), and diplomatic conflicts (Pollins, 1989*b*,*a*). International conflict causes states to become less interdependent generally (Kim and Rousseau, 2005). When states are in conflict they become more focused on relative gains with their adversary, leading to decreases in bilateral trade (Liberman, 1996). Since security crises inhibit trade, formal military alliances promote it (Gowa and Mansfield, 1993, 2004; Mansfield and Bronson, 1997). Gowa (1994) argues that states prefer to trade with allies because

trade creates positive externalities, and states would prefer to provide positive externalities they are unlikely to face in conflict.

While few authors have looked at the impact of trade volumes on transnational internet interconnection, there are some reasons to believe that transnational commerce would affect interconnection. At a basic level demand for interconnection between two networks comes from demand for fast and reliable data transit between the computers in the two networks (Economides et al., 2005; Greenstein, 2020; Norton, 2014). Imagine that a regional internet service provider in Malaysia serves businesses that start to open offices in the Philippines where there is a different internet service provider. Without any direct connection between the networks the Malaysian internet service provider has to send data through intermediaries, which increases the costs and distance their data has to travel, decreasing the speed that data can travel. There are two potential solutions - either directly connect with the internet service provider in the Philippines or find a different intermediary that is closer to the new networks.

This logic can be directly tied to war. For example, if a Ukrainian business closed their offices in Moscow after conflict in Crimea in 2014, they may no longer need an internet service that can exchange data between the two countries. An AS may decide to remove their point of presence in an internet exchange (which they must pay to maintain), if they anticipate decreased demand for data along a route. This might occur regardless of whether there are direct risks from conflict, such as weaponized interdependence, cyberattacks, or payment disruptions. If formal military alliances promote greater non-digital trade, data transit providers may see greater demand for flows, and thus we would observe shifts in the structure of the internet between allies.

Through Business Risk

International conflict creates business risks that cause companies to reduce reliance on certain markets Morrow (1999). Russia's invasion of Ukraine in 2022 demonstrated how conflict creates specific risks to firms that cause businesses to alter how they route data across borders. Two forms of business risks influenced data transit providers to cut off service to Russia - 1.) sanctions that prevent Russian firms from paying for data transit services, and 2.) Russian hackers leveraging international data firms' infrastructures to carry out attacks against their clients.

As Russia prepared in December 2021 to invade Ukraine, Angus King (I-ME) told reporters "I don't think there's a slightest doubt that if there is an invasion or other kind of incursion into

Ukraine, it will start with cyber."[8] At the onset Russia's invasion of Ukraine in February 2022, many observers warned that war created an increased risk of cyberattacks. In the months before the invasion Russian hackers from the GRU used a sophisticated malware called WhisperGate to disrupt Ukrainian government websites.[9] In the hours before the invasion, Russia targeted satellite communications systems owned by U.S.-based internet service provider Viasat.[10]

While Russian cyberattacks primarily targeted Ukrainian systems in 2022, the U.K. government warned that cyberattacks could create significant spillover into systems in Europe due to digital interdependence.[11] This is not a new phenomena - the 2017 NotPetya attacks on the Ukraine spread through Ukrainian tax preparation software, but escalated across private connected networks including banks, government systems, electrical grids, and telecommunication companies in multiple countries.[12] U.S. Secretary of State Anthony Blinken stated that the 2022 attacks against Viasat were designed "to disrupt Ukrainian command and control during the invasion, and those actions had spillover impacts into other European countries."[13] Toby Lewis, head of threat analysis at Darktrace, said that attacks against Ukrainian contractors in Latvia and Lithuania "shows the beginning of the collateral impact of this cyber-conflict on global supply chains."[14] Nevertheless, the greatest risk is to systems in countries that are directly targeted by attacks.

In 2022, two of the companies that operate the internet backbone – Cogent and Lumen - cut off access to their Russian clients. These companies, both headquartered in the United States, own the autonomous systems the 1st and 3rd largest reach on the internet, respectively. Cogent stated that the company did not want its data transit routes to be "used for outbound cyber attacks or

[8]Sanger, David E., and Julian E. Barnes. "U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault." The New York Times, December 20, 2021, sec. U.S. https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.html.

[9]Cybersecurity & Infrastructure Security Agency. "Update: Destructive Malware Targeting Organizations in Ukraine," February 26, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-057a.

[10]Sanger, David E., and Kate Conger. "Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds." The New York Times, May 10, 2022, sec. U.S. https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html.

[11]Sabbagh, Dan. "UK Firms Warned of Russian Cyberwar 'Spillover' from Ukraine." The Guardian, February 23, 2022, sec. Technology. https://www.theguardian.com/technology/2022/feb/23/uk-firms-warned-russia-cyberwar-spillover-ukraine-critical-infrastructure.

[12]Kramer, Andrew E. "Ukraine Cyberattack Was Meant to Paralyze, Not Profit, Evidence Shows." The New York Times, June 28, 2017, sec. World. https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html.; Collins, Keith, and Max de Haldevang. "The Cyber Attack That Knocked out Ukraine This Morning Is Now Going Global." Quartz, June 27, 2017. https://qz.com/1015755/ukraine-cyber-attack-the-petyapetrwrap-ransomware-with-similarities-to-wannacry-is-now-going-global/.

[13]Pearson, James. "Russia Downed Satellite Internet in Ukraine -Western Officials." Reuters, May 11, 2022, sec. Europe. https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/.

[14]Browne, Ryan. "The World Is Bracing for a Global Cyberwar as Russia Invades Ukraine." CNBC, February 25, 2022. https://www.cnbc.com/2022/02/25/will-the-russia-ukraine-crisis-lead-to-a-global-cyber-war.html.

disinformation."[15] Lumen informed its clients that it decided to disconnect because, "We have not yet experienced network disruptions, but given the increasingly uncertain environment and the heightened risk of state action, we took this move to ensure the security of our and our customers' networks, as well as the ongoing integrity of the global Internet."[16]

Transiting data for internet service providers in countries at war also presents economic risks. Conventional economic sanctions meant that data transit firms may not be paid for services or may end up transiting data for sanctioned Russian companies. Cogent emailed its Russian clients on March 3 that "The economic sanctions put in place as a result of the invasion and the increasingly uncertain security situation make it impossible for Cogent to continue to provide you with service" [17] Economic sanctions did not place direct limits on data transit to Russia, but Cogent and Luman are just two among many firms that voluntarily left the Russian market in 2022 due to the economic risks from sanctions.[18] Businesses engaging in markets with sanctions face significant compliance costs and risks that they may be punished if they engage with a business that is under direct sanction.

If data transit creates security externalities due to the risk of cyberattacks, states can more effectively manage them within alliances. One reason why firms reduced data flows to Russia in 2022 is the risk that Russia would leverage their networks to carry out cyberattacks. As Valeriano and Maness (2015) demonstrate, the vast majority of cyberattacks are between rival dyads such as Iran and Israel or Russia and the United States. Since alliances help states manage competition (Leeds, 2003; Owsiak and Frazier, 2014), they reduce the likelihood of cyber conflict within a dyad. The other firm-level risk was sanctions, and allies are unlikely to use economic sanctions as a diplomatic tool even if they would be useful (Drezner, 1999).

Through Weaponized Interdependence Risk

The recent literature on weaponized interdependence draws a direct link between technical structures and international competition. Farrell and Newman (2019) argue that the United States position

[15] Timberg, Craig, Cat Zakrzewski, and Joseph Menn. "A New Iron Curtain Is Descending across Russia's Internet." Washington Post, April 4, 2022. ; Bartz, Diane. "U.S. Firm Cogent Cutting Internet Service to Russia." Reuters, March 4, 2022, sec. Technology. https://www.reuters.com/technology/us-firm-cogent-cutting-internet-service-russia-2022-03-04/.

[16] Lumen Newsroom. "Lumen's Readiness to Meet Global Events." Accessed May 31, 2022. https://news.lumen.com/RussiaUkraine.

[17] Madory, Doug. "Cogent Disconnects from Russia." Kentik Blog, April 4, 2022. https://www.kentik.com/blog/cogent-disconnects-from-russia/.

[18] Katsos, John E., Jason Miklian, and John J. Forrer. "In Light of Russia Sanctions, Consider Your Conditions for Doing Business in Other Countries." Harvard Business Review, March 15, 2022. https://hbr.org/2022/03/in-light-of-russia-sanctions-consider-your-conditions-for-doing-business-in-other-countries.

within the internet architecture enables a vast intelligence gathering program that provides significant security advantages. If this is the case, countries should seek to reduce the amount of data that they transit through an adversary at the onset of a international conflict or as competition increases. Conflict increases both of the risks that Farrell and Newman (2019) identify - that a country will monitor another country's networks for intelligence and exclude them from networks as a sanction.

State pressure to reduce interconnection with rivals and competitors is already occurring - the fear of future conflict is leading the United States to exert control over where internet service providers can route data. In 2017, Facebook and Google proposed investing a minimum of $300 million to build a fiber-optic cable between Los Angeles and Hong Kong. This would have been the second trans-Pacific cable connecting Hong Kong and the United States, but would have had over twelve times the capacity of the existing Asia America Gateway (AAG). The increased capacity would allow tech companies to expand their presence and increase the efficiency of the global internet infrastructure.[19]

In 2019, the U.S. Justice Department cited national security concerns to oppose the bid.[20] In June, 2020 the Department of Justice recommended that the FCC deny the cable license.[21] The recommendation was based on:

> Concerns that PLCN would advance the PRC government's goal that Hong Kong be the dominant hub in the Asia Pacific region for global information and communications technology and services infrastructure, which would increase the share of U.S. internet, data, and telecommunications traffic to the Asia Pacific region traversing PRC territory and PRC-owned or -controlled infrastructure before reaching its ultimate destinations in other parts of Asia.

How the U.S. has approached internet cables to China since 2016 suggests that weaponized interdependence can prompt states to intervene in the internet infrastructure. This mechanism is distinct from firm-level explanations connecting business risk to conflict. At the same time, control over submarine cable landings may not be a strong enough lever to reduce data paths. The

[19] Quigley, Brian. "New Undersea Cable Expands Capacity for Google Asia Pacific Customers and Users." Google Cloud Blog (blog), October 12, 2016.

[20] Strohm, Chris, and Todd Shields. "Justice Department Opposes Google's Undersea Cable From China." Bloomberg.Com, August 28, 2019. https://www.bloomberg.com/news/articles/2019-08-28/justice-department-opposes-google-s-undersea-cable-from-china.; O'Keefe, Kate, Drew FitzGerald, and Jeremy Page. "National Security Concerns Threaten Undersea Data Link Backed by Google, Facebook." Wall Street Journal, August 28, 2019, sec. Politics.

[21] National Security Division. "Team Telecom Recommends That the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States." U.S. Department of Justice, June 17, 2020.

Department of Justice eventually approved the PLCN cable section linking the El Segundo, CA and Toucheng, Taiwan in April 2020, which could then carry data to China.[22]

However, the Snowden leaks demonstrated that states dictating internet interconnection is not necessary for weaponized interdependence to influence data routeing. A key component of the U.S. National Security Agency capabilities was "upstream collection," where the government partnered with AS and IXP operators to collect intelligence from the internet backbone. The United States NSA grew an international intelligence network by "commandeering AT&T's massive infrastructure and using it as a platform to covertly tap into communications processed by other companies."[23] Many countries carry out similar internet intelligence programs, including the Mastering the Internet program in the United Kingdom, Onyx in Switzerland, SORM in Russia, and the Central Monitoring System in India. Whether a partner organization or controlled point on the internet physically routes data creates an intelligence opportunity.

Businesses are aware of how their data is routed, and demanded more control over their data in the aftermath of the Snowden leaks. NTT Communications, one of the largest data carriers in the world, carried out a survey of their customers after the Snowden leaks in 2014. 31% of respondents said that they were moving data to "locations where they know it will be safe," 96% of EU and 92% of US respondents stated they wanted a cloud data service located in their own region. Respondents reported that they cared most about whether a cloud provider could provide guarantees over the physical location of data.[24] When conflict breaks out between two states the value of intelligence increases, which creates risks for data.

Formal alliances reduce the direct risk to data by making cyberattacks and sanctions unlikely. However, numerous cases demonstrate that digital spying - a key part (panopticon) of weaponized interdependence - occurs between allies and outside of conflict, just as between adversaries or during conflict. For instance, the Snowden leaks revealed that the U.S. was spying on NATO allies, including France and Germany.[25] In 2021, Denmark's security services were accused of helping the U.S. National Security Agency spy on European politicians.[26]

[22] U.S. Department of Justice. "Department of Justice Clears on Google's Application to the Federal Communications Commission to Operate a Portion of the Pacific Light Cable Network System," April 8, 2020.

[23] Gallagher, Ryan, and Henrik Moltke. "The NSA's Hidden Spy Hubs in Eight U.S. Cities." The Intercept, June 25, 2018. https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/.

[24] NTT Communications. "NSA After-Shocks: How Snowden Has Changed ICT Decision-Makers' Approach to the Cloud," 2014.

[25] Calamur, Krishnadev. "4 Things To Know About Spying On Allies." NPR, October 28, 2013, sec. Politics & Policy. https://www.npr.org/sections/parallels/2013/10/28/241384089/four-things-to-know-about-spying-on-allies.

[26] BBC News. "NSA Spying Row: Denmark Accused of Helping US Spy on European Officials," May 31, 2021,

If having a formal alliance does not prevent spying via weaponized data flows, and the risk of spying is a significant reason why conflict diminishes data flows, then why should alliances promote data flows? First, the backlash to these cases shows that spying is more costly and less expected among allies than among adversaries. In response to accusations against the U.S. NSA in 2021, French President Emmanuel Macron stated "I want to say it is not acceptable among allies, very clearly" and the Danish Defense Minister Trine Bramsen told the media that "systematic interception of close allies is unacceptable." Spying on allied states is *different* than spying on non-allies, and less acceptable than spying on non-allies. There are normative barriers and costs to spying on allies that states do not have to pay for spying on adversaries, and joining an alliance creates these costs.

Second, while spying among allies may be *normatively* problematic and provoke public ire, it is not likely to result in security advantages, since the likelihood of conflict between allied states is low. Perhaps joining an alliance like NATO does not prevent spying, but it reduces the likelihood of conflict and competition, so spying does not create a negative security externality. Gowa (1994) argues that states prefer to trade with allies because trading creates a positive externality - countries benefit economically from trade and acquire goods that may help them wage war, and so countries would prefer to provide those benefits to states they are unlikely to face in conflict. The Snowden leaks, and the weaponized interdependence argument, demonstrate that data flows can create a potential negative externality by allowing states to collect intelligence (Farrell and Newman, 2019). Future research could evaluate whether information on spying among allies disrupts data flows. The question here is the opposite - whether placing institutional constraints on conflict and competition can promote data flows.

5 Empirical Approach

5.1 Internet Topography

The Center for Applied Internet Data Analysis (CAIDA) at the University of California, San Diego has gathered data about different aspects of the internet architecture since 1998. This paper leverages two CAIDA datasets, *AS Relationships* with peering agreements between systems,[27] and *AS Organizations* that maps autonomous system numbers to organizations.[28] These independent op-

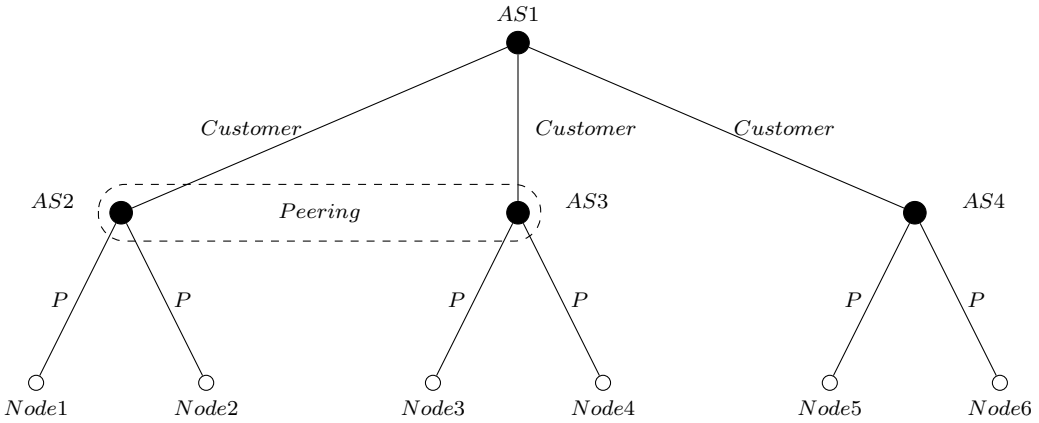
sec. Europe. https://www.bbc.com/news/world-europe-57302806.

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

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

erators agree to exchange data between one another through the Border Gateway Protocol (BGP). This protocol is how requests for information on one system are routed to their destinations.

Figure 1: Representation of AS Relationships



The figure demonstrates the network in the main analysis before it is transferred to the country-country level. Each AS represents one internet service provider, and each $Node$ represents a customer using the internet. The link from $AS2$ to $AS3$ represents a peer-to-peer agreement, where data flows without charge between the operators, while each link with $AS1$ represents a provider-to-customer agreement where data flows with a settlement fee.

Figure 1 helps visualize the two ways that data can be exchanged - peer-to-peer or provider-to-customer. In a peer-to-peer agreement two networks exchange data directly, reducing the cost of delivery by shortening the distance data must travel and limiting intermediaries. These agreements can either be free or paid. Provider-to-customer agreements are agreements for one network to provide access to the internet for fees. Typically network volumes are more asymmetric in provider-to-customer agreements than peer-to-peer.

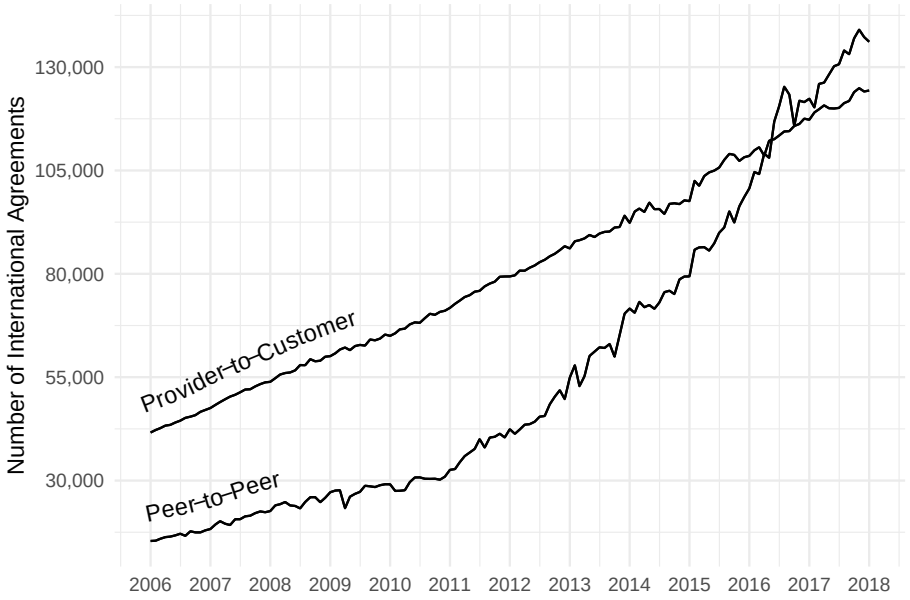
For example, in Figure 1, $AS1$ is a "Tier 1" network which can reach the entire network. Each autonomous system has a customer cone, such as $AS2$ with customer cone $Node1$ and $Node2$, which get their internet access through $AS2$ as a provider. Each autonomous systems has a customer agreement with $AS1$ that allows them to transfer data to any of the other customers of $AS1$. However, $AS2$ and $AS3$ have a peering agreement that allows them to exchange data, thereby bypassing their customer agreements with $AS1$. As demand for data within $AS2$ increases, more ASes may seek to connect with $AS1$ to reach $AS2$. They may also seek to peer directly with $AS2$ if they have access to a physical internet exchange point.

Data can move between any country since every country has at least one agreement. However, when two countries do not have any ASes with a direct link data moves farther to reach its destination and pay every interconnection fee on the way. This means greater latency, higher cost, and less

efficiency. There are opportunities to cut down on the distance between countries if they form more links.

CAIDA collects internet routing data by placing monitors that attempt to contact hosts and record information about how their connection is routed. CAIDA leverages an algorithm to infer the type of agreement (Luckie, Huffaker, Dhamdhere, Giotsas and claffy, 2013). This data is at the autonomous system level - for each month there is a list of agreements between autonomous system numbers that are connected within the Border Gateway Protocol. ASN ownership and location changes ownership over time. CAIDA publishes information about the current ownership of ASes using data from the larger internet registries from January 2004 to the present day. I combine the static snapshots of AS ownership into one dataset with all owners of AS numbers for the entire period. Each registered AS declares a primary country, which I then project to the country-AS level. I merge and clean the two CAIDA datasets to construct the two variable in the analysis - the number of P2P and P2C agreements between two countries (j_i, j_{-i}) in any given month (t). Figure 2 contains the total number of peer-to-peer and customer-to-provider interconnection agreements in the CAIDA dataset, which has increased significantly with the number of internet users. The technical collection process, the cleaning process, and potential biases in this data are discussed further in Appendix Section 2.

Figure 2: International Interconnection Agreements (January 2008-January 2018)



This data is not without limitations. While CAIDA has the largest set of internet monitors of any publicly accessible institution, there may be portions of the internet space where the network has less visibility. This network is only part of internet - data exchange agreements and information about agreement types. However, there is no reason to believe that this measurement error is correlated with the treatments in the paper. CAIDA does not provide information about data exchange prices, data flow capacity within agreements, or the actual data flows. This data at scale has never been available for any academic research. Interconnection agreements are highly correlated with data flows, but the presence of a new agreement merely indicates that data can directly flow between two systems.

The measures used in this paper improves on previous measures of internet interdependence, such as an interaction between the internet penetration rates or number of IP addresses in two countries (Freund and Weinhold, 2002, 2004; Lopez Gonzalez and Ferencz, 2018). The bilateral measure of interdependence in this paper is not derived from whether each member of the dyad is dependent on the internet. Other authors have used Google add patterns or click streams to measure cross-border data flows (Blum and Goldfarb, 2006; Cowgill and Dorobantu, 2014). However, these methods are dependent on the platform that the authors study - add patterns on Google differ from add patterns on Facebook, and there is wide cross-national variation in platform usage. On the other hand, all networks on the internet use the border gateway protocol to move data regardless of where they are on the internet or who they provides services to.

CAIDA's AS-relationships and AS-organizations datasets are one of the standards within the networking literature. Zhuo et al. (2021) used this data to understand the effects of data privacy laws on the internet's structure in Europe. Carisimo et al. (2021) used this data to help identify state-owned internet networks, and Gamero-Garrido (2021) used it to uncover how countries were exposed to data flows. Other authors use this data to understand how networks generally behave (Ward, 2021; Zhou et al., 2019).

5.2 Conflict and Cooperation

Military Conflict

To measure international conflict I use the Militarized Interstate Disputes (MIDs) dataset 4.02, which covers disputes through December 2014 (Maoz et al., 2019). The dyadic dataset records the first and last dates of conflicts in which both states meet the minimum participation criteria. This

analysis considers all physical uses of force between states (MID hostility level 4 and above), but do not include simple displays of force or threats to use force. In the MIDs dataset there are disputes effecting 118 directed-dyads (.6% of total) between January 2008 and December 2015. The MIDs dataset is frequently used to measure the impact of conflict on international trade (Keshk, Pollins and Reuveny, 2004).

Security Cooperation

I use the *Alliance Treaty Obligations and Provisions Project (ATOP)* data on military agreements to measure the impact of alliance and treaty formation on interconnection (Leeds et al., 2002). Version 5.0 of the dataset covers all alliances formed between 1815 and December, 2018. The dataset contains "formal agreements among independent states to cooperate militarily in the face of potential or realized military conflict." These agreements include non-aggression pacts, but not arms sales or military aid agreements unless they include obligations on military cooperation. Between January 2008 and 2018, 72 treaty entries into 30 unique treaties effected a total of 778 dyads (4.1%). Additional information regarding conflict and treaties can be found in Appendix Section 4.

5.3 The Fixed Effects Gravity Model

The general approach for this paper is a fixed-effects gravity model, a common econometric tool in the study of trade (Anderson, 2011; Baldwin and Taglioni, 2006; Carter and Poast, 2020) and online commerce (Cowgill and Dorobantu, 2014). 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 of interconnection agreements between ISPs in two countries as a function of their changing bilateral relationship. While the gravity model typically models imports from a to b, this analysis relies on the more general model of the total volume of trade between a and b.

There are 139 countries in this analysis, each of which is responsible for determining interconnection and internet policy within an internet protocol (IP) space. This results in 19,182 unique dyads over 138 months from January 2008 through January 2019. Of all potential data-transit dyads, 12,406 (65%) never feature an interconnection agreement.

The presence of zero-values for trade is a widely recognized challenge for gravity and fixed effects models. The gravity approach models trade values as logarithms, which are undefined for zero, and

drops all zero values for the dependent variable. There are several issues with this - zero may have substantive importance in itself, and changes between zero and positive values are especially important for interconnection data. This paper adopts the solution from Santos Silva and Tenreyro (2006), modeling raw values for the number of bilateral internet interconnection agreements between ISPs as count data with a Poisson distribution generalized to non-integer data.

This paper uses a high-dimensional fixed effect approach with fixed effects for months and dyads. This specification controls for all time-variant system-levels factors that may affect internet interconnection (new technology, websites, changes in business cycles, etc), along with time-invariant dyadic level factors that may affect the amount of data moving between two countries (distance, contiguous borders, shared language, colonial relationships). [29]. An additional robustness check modeling interconnection only for countries connected by fiber-optic internet cables appears later in this paper.

5.4 Does Data Follow the Flag?

5.5 Main Results

The results demonstrate how international security influences how private firms route data across the globe. New military alliances, which promote conventional trade, reduce the risk of cyberattacks and sanctions, and limit potential negative security externalities from data flows, are associated with significant increases in bilateral data routes. At first glance, the association between military conflict and data paths is confusing - military conflicts seem to open new ways for data to flow between states. However, a robustness check shows that this is due to the large and positive effect of Russia's Ukraine annexations since 2014. While conflict historically reduces trade, the original trade follows the flag thesis argues that conquest should increase trade. Removing the Russia-Ukraine dyad, the relationship between data flow agreements and conflict is either negative (for peer-to-peer) or null (for customer-to-provider). I use a case study to show how control over data routes has been an important part of Russia's Ukraine strategy since 2014, and is used to consolidate control over occupied territories.

[29] Additional results with alternate fixed effects specifications can be found in Appendix Section 5. Appendix Table 2 contains the results with fixed costs for each country in the dyad, rather than the dyad itself. To capture some of the fixed costs of interconnection within a dyad that do not change over time I include the logged distance between the two countries and an indicator for whether they share a border. Appendix Table 3 models time as a series of non-linear spline terms, rather than as an intercept term, and contains fixed effects for the dyad. Finally, Appendix Table 4 contains the results with splines for time and fixed effects for the two countries in the dyad, along with logged distance and contiguity. None of the results change for these specifications.

There are two types of data exchange agreements that internet service providers can enter into - provider-to-customer (P2C) and peer-to-peer (P2P). The P2C agreements tend to be more asymmetric in their data flows, with the customer demanding data from the provider and agreeing to pay a settlement fee. Conversely, P2P agreements occur when there is equal demand for data transiting from both networks and exchange typically occurs without fees. While networks can interconnect two distinct ways, international conflict and cooperation do not have heterogeneous effects between different interconnection methods.

Table 1: Effects of Security Cooperation and Conflict on Interconnection

Dependent Variable:	**Provider-to-Customer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.185***	0.101	0.167***	0.173***
	(0.054)	(0.133)	(0.049)	(0.049)
Observations	374,544	374,328	591,840	591,552
Dependent Variable:	**Peer-to-Peer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.622***	-0.475***	0.441***	0.444***
	(0.087)	(0.156)	(0.153)	(0.153)
Observations	313,848	313,632	625,824	625,536
Fixed-effects				
Dyad	Yes	Yes	Yes	Yes
Month	Yes	Yes	Yes	Yes

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

The results for conflict and interconnection are contained in Table 1. MIDs cover all dyads through December 2014. Surprisingly, military conflict appears to be associated with *positive* effects, while military conflict suppressed most forms of trade (Pollins, 1989*a*; Glick and Taylor, 2010; Anderton and Carter, 2001). An active militarized interstate dispute is associated with a weakly significant 9.4% *increase* in provider-to-customer internet interconnection paths and a statistically robust 67.0% *increase* in peer-to-peer interconnection paths.

Understanding international conflict's impact on data flows faces a familiar challenge as conventional trade - countries that are *a priori* likely to enter into conflict are unlikely to be trading with one another. Among the 83 undirected-dyads facing a militarized interstate dispute, 58 have

no data exchange agreements between their internet spaces. The bilateral relationships with a use of force and the largest data flows, which exert the greatest force on the results, are in Table 2. The Russia-Ukraine dyad has ten times the number of agreements between internet service providers as the next most significant conflict dyad. The remaining conflicts between dyads with significant data flows include a series of shows of force by Russia between November 2012 and December 2014 and a land dispute between Thailand and Cambodia in 2014.

Table 2: Top-12 Countries with MIDs and Data Flows

Dyad	Avg. Agreements	Dyad	Avg. Agreements
RU-UA	166.96	CN-JP	10.44
LT-RU	16.05	PK-US	8.90
KH-TH	14.58	IN-IT	8.05
KZ-RU	14.32	FR-IL	7.01
CN-RU	13.22	CN-KR	6.02
JP-RU	11.20	GE-RU	3.82

This table contains the twelve dyads with MIDS with the greatest amount of data agreements during their non-conflict months. The average includes both peer-to-peer and provider-to-customer agreements.

The third column in Table 1 contains the result for militarized interstate disputes *excluding* the Russia-Ukraine dyad entirely. While there was a positive and significant relationship between conflict and provider-to-customer in the whole sample, the results in the RU-UA-excluded sample are insignificant. Furthermore, militarized interstate disputes now have a *negative* (-26.3%) impact on peer-to-peer data flows. The Russia-Ukraine dyad is unique for two reasons - first, because it is a conflict dyad with significant data routes across it. Second, it is one of the only cases in the study period where one state annexed territory from another. The next section of this paper shows why territorial annexation should lead to increases in data pathways, in line with the traditional "trade follows the flag" hypothesis that colonialism promotes trade.

The second column in Table 1 addresses the relationship between new security agreements and data exchange agreements. New agreements came into effect between 291 dyads between 2008 and 2019. An alliance between two states is associated with a positive and significant increase in both provider-to-customer (24.5%) and peer-to-peer (72.1%) data exchange agreements. These results do not change in the fourth column, where the analysis excludes the Russia-Ukraine dyad.

This result is in line with authors who argue that military alliances promote trade and integration between states (Gowa and Mansfield, 1993, 2004; Gowa, 1994; Mansfield and Bronson, 1997). This paper previously posited three mechanisms for how alliances could promote data flows - increased non-digital trade, reduced business risks from cyberattacks and sanctions, and decreased risk from

weaponized interdependence.

Since this data is measured at the monthly level, immediate increases in data routes due to increases in trade generally are less likely. More refined data on bilateral trade at the monthly level might help disentangle whether data routes are increasing due to alliances because of increases in trade. Spying among allies is commonplace, which might indicate that alliances do little to assuage concerns regarding weapoinzed interdependence. However, as previously discussed, alliances do reduce the risk *from* data siphoned by another state, even if they do not reduce the risk that data *will* be siphoned by another state. The United States, for example, has less to fear from a close ally like Germany accessing data than from adversaries like China or Russia.

5.6 Selected Sample: Cable Networks

One potential concern is the assumption that any country is able to exchange data with any country. However, there may also be fixed costs to internet exchange that limit the number of potential dyads that can be affected by international treaties or conflict. One important fixed cost is fiber-optic cables that carry approximately 99% of trans-continental data traffic (Bueger and Liebetrau, 2021; Carter, 2009; Starosielski, 2015).[30] In 2014, cables in the Mediterranean sea cost approximately $90,000 per kilometer, and the construction of large intercontinental cables like SEA-ME-WE 3 can take up to three years to build.[31]

I collect data on submarine and terrestrial cable networks to account for this potential bias. For data on current submarine cables, I use information from Telegeography,[32] and for data on unused or "dark" cables, I use data from the Submarine Cable Almanac, which began reporting on cable networks in 2011.[33] Countries are included if they are both partners to a submarine cable that meets at a shared landing point. All contiguous countries are also selected due to un-mapped terrestrial fiber networks. Finally, I include three of the largest terrestrial fiber networks - the European Backbone, the TEA Cable, and the TKK Eurasia Highway.[34]

Limiting the analysis to only countries with an internet cable link in January 2006 reduces the

[30] Griffiths, James. "The Global Internet Is Powered by Vast Undersea Cables. But They're Vulnerable." CNN, July 26, 2019.

[31] Neal, Ryan W. "Underwater Internet Cables: 'Submarine Cable Map' Shows How The World Gets Online." International Business Times, March 5, 2014. https://www.ibtimes.com/underwater-internet-cables-submarine-cable-map-shows-how-world-gets-online-1559604.

[32] TeleGeography. "Submarine Cable Map." Submarine Cable Map. https://www.submarinecablemap.com/.

[33] Submarine Telcoms Forum. "Submarine Cable Almanac." https://subtelforum.com/products/submarine-cable-almanac/.

[34] See Appendix Section 3 for a discussion on how this measure is constructed.

number of potential dyads from 20,880 to 4,018, and reduces the prevalence of all-zero dyads from 65% to 29%. Additionally, the percentage of dyads affected by changes in alliance status increases from 4.1% to 8.4%, and the percentage of dyads affected by changes in conflict status increases from .6% to 2.6%. The dyads with the greatest interconnection that are excluded are the United States with Switzerland, Sweden, Poland, South Africa, and Austria. Table 3 contains the results for the main analysis limiting only to dyads with fixed interconnection costs by January 2008.

Table 3: Effects of Security Cooperation and Conflict on Interconnection for Dyads Linked in 2006

Dependent Variable:	**Provider-to-Customer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.195***	0.093	0.185***	0.193***
	(0.057)	(0.138)	(0.051)	(0.051)
Observations	197,290	197,072	292,608	292,320
Dependent Variable:	**Peer-to-Peer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.623***	-0.523***	0.479***	0.482***
	(0.090)	(0.159)	(0.175)	(0.175)
Observations	166,552	166,334	275,904	275,616
Fixed-effects				
Dyad	Yes	Yes	Yes	Yes
Month	Yes	Yes	Yes	Yes

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

The relationship between military treaties and both peer-to-peer and provider-to-customer data exchange remains positive and significant. Similar to the unrestricted sample results in Table 1, militarized interstate disputes have a positive and significant association with provider-to-customer data exchange and peer-to-peer data interconnection. Removing the Russia-Ukraine conflict, the positive relationship between militarized interstate disputes and provider-to-customer data exchange is now insignificant, and between peer-to-peer agreements is now negative and significant.

6 Territorial Conquest and the Internet

Is the positive relationship between military conflict and data routes evidence that data does not follow the flag? Despite the risk that war creates due to increased cyberattacks and sanctions, blunted trade, and weaponized interdependence, the data appears to continue flowing. However, the positive association between interconnection and conflict is driven by the Russia-Ukraine conflict in 2014, and the conflict demonstrates how data can directly follow the flag.

What happens to the internet in one territory when another country takes it over? While conflict between states reduces trade, the original "trade follows the flag" hypothesis is that states can use military conquest and colonialism to promote trade in other territories (Berger et al., 2013; Mitchener and Weidenmier, 2008). Appendix Section 6 contains a robustness check where the affected dyad is dropped from the analysis sequentially. Dropping the Russia-Ukraine dyad from the analysis changes the coefficient in the peer-to-peer results to from positive and significant to negative and significant, and changes the provider-to-customer results from weakly significant to insignificant. The relationship between peer-to-peer data routes and international conflict is not affected by removing any other dyad. Dropping the Afghanistan-Pakistan dyad also changes the provider-to-customer results from weakly significant to insignificant. Dropping any one dyad does not affect the results for alliances.

In the aftermath of protests in February 2014, the Ukrainian parliament removed pro-Russia Ukrainian President Viktor Yanukovych from office. Afterwards, Russia leveraged internal divisions in Ukraine to promote conflict in Crimea and Donbas, eventually leading to a Russian invasion and annexation of Crimea in March 2014. Conflict between Ukrainian and Russian-backed forces continued in Donbas from 2014, and in February 2022 Russia waged a full-scale invasion of Ukraine, consolidating control over Donbas and western Ukraine.

The Russian annexation of Crimea in 2014 immediately changed how data flowed through and out of Ukraine. First, numerous autonomous systems changed their registration from Ukraine to Russia. This includes Bospor-Telecom (AS42238), CrimeaCom (AS28761), and CrimeaCom South (AS48086). In the short term, this means that interconnection pathways for these ASes with systems in Ukraine are re-assigned from domestic to international. Instead of interconnection with another autonomous system in Ukraine, many systems were now interconnecting with systems Russia (Fontugne, Ermoshina and Aben, 2020). In August 2014, Russia spent $11-25 million to build

new submarine fiber-optic infrastructure to carry Crimean data through Russian information space, increasing Russia's digital foothold.[35] Rostelecom, a Russian state-owned internet service provider, and local partner "Miranda Media," provided the Crimean region with access to data flows. With a new cable in place, the fastest and least expensive way for data to leave Crimea was through Russia.

Limonier et al. (2021) note that, in the aftermath of the 2014 invasion, eastern Ukrainian cyberspace "sits at the interface of Ukraine and Russia but has been relegated to the periphery of both networks; it is marginalized from the Ukrainian network but not fully integrated into the Russian network." Russian control over the physical infrastructure provides political benefits and control. Russia leveraged access to Crimean internet space to consolidate its power in the region with Russian-style information control techniques.[36]

Russia continued shaping the direction of Ukrainian data flows through its invasion in 2022. The internet and tech platforms have been an integral part of both the Russian invasion of Ukraine and the Ukrainian resistance.[37] In April, Russian media reported on state-building enterprises in eastern Ukraine, which included internet infrastructure.

> More than 200 stores have resumed work in the liberated territories of the DPR (Donetsk People's Republic). In Volnovakha and Novotroitsk, work was carried out to set up the equipment of a local Internet access provider. In Kremenevka, Privolnoye, Andreevka and Bakhchevik, local providers have been provided with a communication channel for accessing the Internet.[38]

In May 2022, Russian forces effectively overtook the internet infrastructure throughout its occupied territories and began to route internet traffic out of Ukraine and into Russia by disrupting terrestrial internet fiber cables in Kherson. This prevented internet operators from routing towards

[35] Moss, Sebastian. "How Russia Took over the Internet in Crimea and Eastern Ukraine." Data Center Dynamics, February 25, 2022. https://www.datacenterdynamics.com/en/analysis/how-russia-took-over-the-internet-in-crimea-and-eastern-ukraine/.; Sherman, Justin. "Cord-Cutting, Russian Style: Could the Kremlin Sever Global Internet Cables?" Atlantic Council (blog), January 31, 2022. https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/.

[36] Mirani, Leo. "Crimea Just Switched over to the Russian Internet." Quartz, August 1, 2014. https://qz.com/243619/crimea-just-switched-over-to-the-russian-internet/; Cox, Joseph. "Russia Built an Underwater Cable to Bring Its Internet to Newly Annexed Crimea." Vice (blog), August 1, 2014. https://www.vice.com/en/article/ypw35k/russia-built-an-underwater-cable-to-bring-its-internet-to-newly-annexed-crimea.

[37] Feldstein, Steven. "4 Reasons Why Putin's War Has Changed Big Tech Forever." Foreign Policy (blog), March 29, 2022. https://foreignpolicy.com/2022/03/29/ukraine-war-russia-putin-big-tech-social-media-internet-platforms/.

[38] "Интернет в Волновахе и Открытие Магазинов в Освобожденных Землях. Обзор Событий в ДНР 19 Апреля," April 19, 2022. https://dan-news.info/defence/internet-v-volnovahe-i-otkrytie-magazinov-v-osvobozhdennyh-zemljah.-obzor-sobytij/?lang=ru.

Europe, which U.K.-based mobile operator Vodafone described as an intentional blackout to create dependence on Russian cyberspace. Hours later, regional internet provider Skynet regained service, but routed data through Russian services Rostelecom and Miranda instead of Ukrainian digital providers.[39] Ryan Gallagher from *Bloomberg* argued in June 2022 that "Control of Ukrainian Internet Is New Focus in Russian Invasion" due to the significant resources the Russian government diverted to overtake Ukrainian digital space.[40]

London-based internet research organization NetBlocks stated that, due to changes in internet routing from Ukrainian internet service providers, the internet in eastern Ukraine is "likely now subject to Russian internet regulations, surveillance, and censorship."[41] Anna Gross from the *Financial Times* wrote that Russian control over the internet infrastructure was "making Ukrainians' data vulnerable to interception and censorship by the Kremlin".[42] Victor Zhora, deputy chief of Ukraine's information protection service, stated in an interview that "The enemy's objective is to strip our people's access to true information, making only Russian propaganda available."[43]

In line with the "trade follows the flag" hypothesis, if conflict results in conquest, data appears to flow to the conqueror. The same way that any colonial occupier might exert control over economic networks in new territories, Russia exerted control over how data flows out of Ukraine. However, instead of diverting natural resources from a conquered territory or forcing it to sell goods and services, Russia diverted data from newly conquered regions in Ukraine.

7 Contributions

The internet was supposed to lessen state power by bringing about a global network sustained by the private sector, disrupting traditional sovereignty and laws (Daskal, 2015; Froomkin, 1997; Johnson and Post, 1996; Kobrin, 2001; Svantesson, 2017; Swire, 1998). While the internet's structure influences international economic and military competition, it is negotiated by individual private

[39] NetBlocks. "Internet Disruptions Registered as Russia Moves in on Ukraine," February 24, 2022. https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.

[40] Gallagher, Ryan. "Control of Ukrainian Internet Is New Focus in Russian Invasion." Bloomberg.Com, June 6, 2022. https://www.bloomberg.com/news/newsletters/2022-06-08/ukrainian-internet-is-focus-of-new-fight-after-russian-invasion.

[41] Reuters. "Russia Reroutes Internet Traffic in Occupied Ukraine to Its Infrastructure." Reuters, May 2, 2022, sec. Europe. https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/.

[42] Gross, Anna. "Russian Forces Usurp Ukrainian Internet Infrastructure in Donbas." Financial Times, May 5, 2022. https://www.ft.com/content/969ac0a8-c0bf-4114-9029-7f75e7895845.

[43] Gallagher, Ryan. "Control of Ukrainian Internet Is New Focus in Russian Invasion." Bloomberg.Com, June 6, 2022. https://www.bloomberg.com/news/newsletters/2022-06-08/ukrainian-internet-is-focus-of-new-fight-after-russian-invasion.

firms. The internet is a distributed system sustained by tens of thousands of operators who choose where and when to exchange data, but these operators exist within national boundaries.

This paper provides evidence that data does follow the flag. New military treaties, which do little to prevent states from weaponizing data flows for intelligence, promote data pathways across states. This may be because treaties help promote non-digital trade, limit the risk from sanctions and cyberattacks, and blunt the negative security externality from weaponized interdependence, are associated with positive and significant increases in data pathways between states. This helps demonstrates the source of risk in weaponized interdependence - spying is less of a business risk when it does not come with a security externality. All else equal, internet service operators would prefer to exchange data in a country that is allied to one in a country that is not.

At first glance military disputes between states appear to *increase* data pathways between states. However, the trade follows the flag literature has always distinguished between conflict that leads to annexation (which increases trade) and conflict between states generally (which decrease trade). Russia-Ukraine conflict since 2014 is responsible for the positive relationship between international conflict and data structures. Removing this dyad from the analysis changes the relationship between conflict and flows from positive to either negative or indistinguishable from zero. The Russia-Ukraine dyad is unique for two reasons - it is a conflict dyad with significant data pathways, and it is a conflict dyad that resulted in annexed territory. This paper presents a brief case study to show how control over physical territory allows control over data routes due to key investments in infrastructure. Russia undertook this expensive economic project because Russia's control over physical data routes data to control over Ukrainian internet space, facilitating information control in new territory.

Several lines of research have not been addressed in this paper. If security treaties increase data interconnection, and data interconnection facilitates the digital economy, technology or internet-dependent firms may lobby for international cooperation. This line of thinking is behind the commercial peace argument (Gartzke, Li and Boehmer, 2001; Gartzke, 2007). Furthermore, while new military treaties may promote data transit between countries, allegations of spying might undermine trust and interdependence. This paper does not test which of the specific mechanisms behind the trade follows the flag argument drive the results. However, it explains that conflict might reduce data flows due to 1.) an effect on non-digital trade, 2.) risk to businesses from sanctions and cyberattacks, or 3.) weaponized interdependence. Improvements to data on international trade, cyberattacks, and sanction risks could help disentangle these mechanisms, and additional work on how

spying affects commerce within alliances could help understand how weaponized interdependence shapes the global economy.

The global internet structure is pushed and pulled by international security - countries' security relationships influence how internet service providers behave at an elemental level. This structure has significant implications for economic growth and the health of the digital economy. However, it is not simply a result of network operators making efficient decisions about distributing data across networks. The dominant narrative that the internet was "un-territorial" ignored how the individual networks that create the internet manage risk in the presence of international conflict and cooperation.

References

Abbate, Janet. 1999. *Inventing the Internet*. Inside Technology Cambridge, Mass: MIT Press.

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

Anderton, Charles H. and John R. Carter. 2001. "The Impact of War on Trade: An Interrupted Times-Series Study." *Journal of Peace Research* 38(4):445–457.

Baake, Pio and Thorsten Wichmann. 1999. "On the Economics of Internet Peering." *NETNOMICS* 1(1):89–105.

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.

Berger, Daniel, William Easterly, Nathan Nunn and Shanker Satyanath. 2013. "Commercial Imperialism? Political Influence and Trade during the Cold War." *American Economic Review* 103(2):863–896.

Blum, Bernardo S. and Avi Goldfarb. 2006. "Does the Internet Defy the Law of Gravity?" *Journal of International Economics* 70(2):384–405.

Bueger, Christian and Tobias Liebetrau. 2021. "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network." *Contemporary Security Policy* 42(3):391–413.

Cairncross, Frances. 1997. *The Death of Distance: How the Communications Revolution Will Change Our Lives*. Boston, Mass: Harvard Business School Press.

Carisimo, Esteban, Alexander Gamero-Garrido, Alex C. Snoeren and Alberto Dainotti. 2021. Identifying ASes of State-Owned Internet Operators. In *Proceedings of the 21st ACM Internet Measurement Conference*. Virtual Event: ACM pp. 687–702.

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

Carter, David B, Rachel L Wellhausen and Paul K Huth. 2019. "International Law, Territorial Disputes, and Foreign Direct Investment." *International Studies Quarterly* 63(1):58–71.

Carter, Lionel, ed. 2009. *Submarine Cables and the Oceans: Connecting the World*. Number no. 31 *in* "UNEP-WCMC Biodiversity Series" Cambridge: UNEP World Conservation Monitoring System ; International Cable Protection Committee.

Chakravorti, Bhaskar and Ravi Shankar Chaturvedi. 2020. "Which Countries Were (And Weren't) Ready for Remote Work?" *Harvard Business Review* .

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.

Chavula, Josiah, Amreesh Phokeer, Agustin Formoso and Nick Feamster. 2017. Insight into Africa's country-level latencies. In *2017 IEEE AFRICON: Science, Technology and Innovation for Africa, AFRICON 2017*. Institute of Electrical and Electronics Engineers Inc. pp. 938–944.

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.

Corrales, Javier and Frank Westhoff. 2006. "Information Technology Adoption and Political Regimes." *International Studies Quarterly* 50(4):911–933.

Cowgill, Bo and Cosmina Dorobantu. 2014. "Worldwide Gravity in Online Commerce.".

Czernich, Nina, Oliver Falck, Tobias Kretschmer and Ludger Woessmann. 2011. "Broadband Infrastructure and Economic Growth*." *The Economic Journal* 121(552):505–532.

Daskal, Jennifer. 2015. "The Un-Territoriality of Data." *Yale Law Journal* 125(2).

Davis, Christina L. and Sophie Meunier. 2011. "Business as Usual? Economic Responses to Political Tensions." *American Journal of Political Science* 55(3):628–646.

DeNardis, Laura. 2012. "Hidden Levers of Internet Control." *Information, Communication & Society* 15(5):720–738.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press.

Drezner, Daniel W. 1999. *The Sanctions Paradox: Economic Statecraft and International Relations*. Number 65 *in* "Cambridge Studies in International Relations" Cambridge [England] ; New York: Cambridge University Press.

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

Economides, Nicholas, Sumit K. Majumdar, Ingo Vogelsang and Martin E. Cave. 2005. The Economics of the Internet Backbone. In *Handbook of Telecommunications Economics*. Vol. 2 Elsevier.

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

Feamster, Nick, Jared Winick and Jennifer Rexford. 2004. A Model of BGP Routing for Network Engineering. In *SIGMETRICS '04/Performance '04*. p. 12.

Fontugne, Romain, Ksenia Ermoshina and Emile Aben. 2020. The Internet in Crimea: A Case Study on Routing Interregnum. In *2020 IFIP Networking Conference*. Paris, France: .

Freund, Caroline and Diana Weinhold. 2002. "The Internet and International Trade in Services." *American Economic Review* 92(2):236–240.

Freund, Caroline L. and Diana Weinhold. 2004. "The Effect of the Internet on International Trade." *Journal of International Economics* 62(1):171–189.

Froomkin, A. Michael. 1997. The Internet as a Source of Regulatory Arbitrage. SSRN Scholarly Paper ID 2718515 Social Science Research Network Rochester, NY: .

Gamero-Garrido, Alexander. 2021. Transit Influence of Autonomous Systems: Country-Specific Exposure of Internet Traffic PhD thesis University of California San Diego.

Gartzke, Erik. 2007. "The Capitalist Peace." *American Journal of Political Science* 51(1):166–191.

Gartzke, Erik, Quan Li and Charles Boehmer. 2001. "Investing in the Peace: Economic Interdependence and International Conflict." *International Organization* 55(2):391–438.

Glick, Reuven and Alan Taylor. 2010. "Collateral Damage: Trade Disruption and the Economic Impact of War." *The Review of Economics and Statistics* 92(1):102–127.

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

Gowa, Joanne and Edward D. Mansfield. 1993. "Power Politics and International Trade." *The American Political Science Review* 87(2):408–420.

Gowa, Joanne and Edward D. Mansfield. 2004. "Alliances, Imperfect Markets, and Major-Power Trade." *International Organization* 58(4):775–805.

Greenstein, Shane. 2020. "The Basic Economics of Internet Infrastructure." *Journal of Economic Perspectives* 34(2):192–214.

Grinberg, Mariya. 2021. "Wartime Commercial Policy and Trade between Enemies." *International Security* 46(1):9–52.

Grove, Stijn and Judith de Lange. 2021. 2021 State of the Dutch Data Hub. Technical report Digital Gateway to Europe.

Guillén, Mauro F. and Sandra L. Suárez. 2005. "Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-National Internet Use." *Social Forces* 84(2):681–708.

Gupta, Arpit, Matt Calder, Nick Feamster, Marshini Chetty, Enrico Calandro and Ethan Katz-Bassett. 2014. Peering at the Internet's Frontier: A First Look at ISP Interconnectivity in Africa. In *Passive and Active Measurement*, ed. Michalis Faloutsos and Aleksandar Kuzmanovic. Lecture Notes in Computer Science Cham: Springer International Publishing pp. 204–213.

Hall, Chris, Ross Anderson, Richard Clayton, Evangelos Ouzounis and Panagiotis Trimintzios. 2011. Resilience of the Internet Interconnection Ecosystem. Technical report European Network and Information Security Agency.

Headrick, Daniel R. 1988. *The Tentacles of Progress: Technology Transfer in the Age of Imperialism, 1850-1940*. New York: Oxford University Press.

Henisz, Witold J. and Bennet A. Zelner. 2001. "The Institutional Environment for Telecommunications Investment." *Journal of Economics & Management Strategy* 10(1):123–147.

Hills, Jill. 2002. *The Struggle for Control of Global Communication: The Formative Century*. The History of Communication Urbana: University of Illinois Press.

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

Johnson, David R. and David Post. 1996. "Law and Borders: The Rise of Law in Cyberspace." *Stanford Law Review* 48(5):1367–1402.

Keohane, Robert Owen and Joseph S. Nye. 1977. *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown.

Keshk, Omar M. G., Brian M. Pollins and Rafael Reuveny. 2004. "Trade Still Follows the Flag: The Primacy of Politics in a Simultaneous Model of Interdependence and Armed Conflict." *The Journal of Politics* 66(4):1155–1179.

Kim, Hyung Min and David L. Rousseau. 2005. "The Classical Liberals Were Half Right (or Half Wrong): New Tests of the 'Liberal Peace', 1960-88." *Journal of Peace Research* 42(5):523–543.

Kobrin, Stephen J. 2001. "Territoriality and the Governance of Cyberspace." *Journal of International Business Studies* 32(4):687–704.

Leeds, Brett Ashley. 2003. "Do Alliances Deter Aggression? The Influence of Military Alliances on the Initiation of Militarized Interstate Disputes." *American Journal of Political Science* 47(3):427–439.

Leeds, Brett Ashley, Jeffrey M. Ritter, Sara McLaughlin Mitchell and Andrew G. Long. 2002. "Alliance Treaty Obligations and Provisions, 1815-1944." *International Interactions* 28:237–260.

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

Liberman, Peter. 1996. "Trading with the Enemy: Security and Relative Economic Gains." *International Security* 21(1):147–175.

Limonier, Kevin, Frédérick Douzet, Louis Pétiniaud, Loqman Salamatian and Kave Salamatian. 2021. "Mapping the Routes of the Internet for Geopolitics: The Case of Eastern Ukraine." *First Monday* .

Long, Andrew G. 2008. "Bilateral Trade in the Shadow of Armed Conflict." *International Studies Quarterly* 52(1):81–101.

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

Luckie, Matthew, Bradley Huffaker, Amogh Dhamdhere, Vasileios Giotsas and kc claffy. 2013. AS Relationships, Customer Cones, and Validation. In *Proceedings of the 2013 Conference on Internet Measurement Conference*. Barcelona Spain: ACM pp. 243–256.

Mansfield, Edward D. and Rachel Bronson. 1997. "Alliances, Preferential Trading Arrangements, and International Trade." *The American Political Science Review* 91(1):94–107.

Maoz, Zeev, Paul L. Johnson, Jasper Kaplan, Fiona Ogunkoya and Aaron Shreve. 2019. "The Dyadic Militarized Interstate Disputes (MIDs) Dataset Version 3.0: Logic, Characteristics, and Comparisons to Alternative Datasets." *Journal of Conflict Resolution* 6(3):811–835.

McKnight, Lee W. and Joseph P. Bailey. 1998. *Internet Economics*. MIT Press.

Milner, Helen V. 2006. "The Digital Divide: The Role of Political Institutions in Technology Diffusion." *Comparative Political Studies* .

Mitchener, Kris James and Marc Weidenmier. 2008. "Trade and Empire." *The Economic Journal* 118(533):1805–1834.

Morrow, James D. 1999. "How Could Trade Affect Conflict?" *Journal of Peace Research* 36(4):481–489.

Mueller, Milton, Andreas Schmidt and Brenden Kuerbis. 2013. "Internet Security and Networked Governance in International Relations." *International Studies Review* 15(1):86–104.

Norton, William B. 2014. *The 2014 Internet Peering Playbook: Connecting to the Core of the Internet*. 2014 ed ed. Palo Alto, Calif.: DrPeering Press.

O'Hara, Kieron and Wendy Hall. 2021. *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. New York: Oxford University Press.

Owsiak, Andrew P. and Derrick V. Frazier. 2014. "The Conflict Management Efforts of Allies in Interstate Disputes1." *Foreign Policy Analysis* 10(3):243–264.

Pollins, Brian M. 1989*a*. "Conflict, Cooperation, and Commerce: The Effect of International Political Interactions on Bilateral Trade Flows." *American Journal of Political Science* 33(3):737–761.

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

Price, Monroe Edwin, Stefaan G. Verhulst and Stefaan Verhulst. 2005. *Self-Regulation and the Internet*. Kluwer Law International B.V.

Roller, Lars-Hendrik and Leonard Waverman. 2001. "Telecommunications Infrastructure and Economic Development: A Simultaneous Approach." *American Economic Review* 91(4):909–923.

Santos Silva, J. M. C. and Silvana Tenreyro. 2006. "The Log of Gravity." *The Review of Economics and Statistics* 88(4):641–658.

Savage, I. Richard and Karl W. Deutsch. 1960. "A Statistical Model of the Gross Analysis of Transaction Flows." *Econometrica* 28(3):551–572.

Sivetc, Liudmila. 2021. "Controlling Free Expression "by Infrastructure" in the Russian Internet: The Consequences of RuNet Sovereignization." *First Monday* .

Slaughter, Anne-Marie. 2017. *The Chessboard and the Web: Strategies of Connection in a Networked World*. New Haven: Yale University Press.

Starosielski, Nicole. 2015. *The Undersea Network*. Sign, Storage, Transmission Durham: Duke University Press.

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.

Svantesson, Dan Jerker B. 2017. *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press.

Swire, Peter P. 1998. "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet." *University of Pennsylvania Law Review* 253:1975–2005.

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

van Dijk, Jan and Kenneth Hacker. 2003. "The Digital Divide as a Complex and Dynamic Phenomenon." *The Information Society* 19(4):315–326.

van Eeten, Michel JG and Milton Mueller. 2013. "Where Is the Governance in Internet Governance?" *New Media & Society* 15(5):720–736.

Ward, Jonathan A. 2021. "Dimension-Reduction of Dynamics on Real-World Networks with Symmetry." *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 477(2251):20210026.

Winseck, Dwayne Roy and Robert M. Pike. 2007. *Communication and Empire: Media, Markets, and Globalization, 1860-1930*. Durham: Duke University Press.

Zhou, Mingyang, Xiaoyu Li, Wenman Xiong and Hao Liao. 2019. "Coevolution of Synchronization and Cooperation in Real Networks." *International Journal of Modern Physics C* 30(07):1940012.

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).

Does Data Follow the Flag?
Supplementary Appendix

Last modified: October 20, 2022

Contents

1 Models

All of the analyses in this paper are carried out using the R Statistical Computing language. This section provides some clarification to the discussion in the main text. All models were carried out using the `fixest` package,[1] which is optimized for large datasets.

Standard Errors I use robust standard errors, clustered at the directed dyad level. This allows the model to deal with correlation between the observations for the same dyad over time. This standard errors approach is also used for the alternative monadic fixed effects specification.

Gravity Model The general approach for this paper is the gravity model, which is a common economics and political method to study trade (Carter and Poast, 2020). 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 61,752 potential dyads. However, to reduce the dimensionality of the data I only include IP spaces representing areas with a population greater than two million. This data is in an directed dyad format, where the dependent variable modeled as the number of interconnection agreements between the countries in the dyad, and the dataset contains a symmetric pair for the number of interconnection agreements between the countries in the other direction (Anderson, 2011; Baldwin and Taglioni, 2006).

Control Data For robustness in Section 6 I model alternative fixed effects specifications form the main paper. When including monadic fixed effects instead of dyadic fixed effects I include control data on whether the two countries are contiguous and their distance. All else equal, two countries that are contiguous should feature more interconnection due to terrestrial fiber networks, and two states further apart should trade less. Data on contiguity and distance come from the *Dynamic Gravity Dataset*, which provides annual data for countries and country-pairs for 285 countries and territories (Gurevich and Herman, 2018).

2 Internet Interconnection

2.1 Overview

The Center for Applied Internet Data Analysis (CAIDA) at the University of California, San Diego has gathered data about different aspects of the internet architecture since 1998. This paper leverages two CAIDA datasets, *AS Relationships* with peering agreements between systems,[2] and *AS Organizations* that maps autonomous system (AS) numbers to organizations.[3] These independent operators form agreements to exchange data between one another through 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. These measurements are typically taken between the 1st and 5th of the month.]

2.2 Sources of Potential Bias

CAIDA's ASN to Organization data, which allows researchers to map autonomous systems onto countries, is only updated every three months, while the interconnection data is updated every month. This can lead to situations where an interconnection is erroneously assigned to one country

[1] Berge, Laurent, Sebastian Krantz, and Grant McDermott. Fixest: Fast Fixed-Effects Estimations (version 0.10.0), 2021. https://CRAN.R-project.org/package=fixest.

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

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

when the registration had already changes. This could potentially occur for two months if the registration changed in the 30 days after the previous ASN to Organization dataset was published. To correct against this bias, I purchased a subscription from Big Data Cloud (api.bigdatacloud.net), and ran it on all current ASN numbers to get registration details for all currently active systems. I then assign a new start and end date to the CAIDA dataset based on the individual registration data to get the precise date that it was registered. Many historical observations also contain information about when the registration was last changed - in these cases I alter the registration date to reflect the stated changed date. However, this information is not contained in all observations.

While this is a potential source of measurement error, I have no reason to believe that this would be biased in any particular direction. It is possible that delays in assigning autonomous systems to countries might bias against interconnection to countries that are experiencing disproportionate increases in interconnection overall. There is also more measurement error in the peering data than the transit interconnection data, since networks do not have to announce their peers to their providers (Zhuo, Huffaker, Claffy and Greenstein, 2020).

One significant challenge with this data is that networks may have a presence in multiple countries, which would not necessarily appear in this dataset. For instance, an company based in the US may have an AS with endpoints outside of the US. This is a problem for only the largest systems, since the vast majority of ASes are geographically bounded to a single area. Groups headquartered in one country may also choose to register an AS in their home region rather than the region where the AS operates. I compare the registered country with the geographic spread of IP addresses, and change the location of autonomous systems which control no IP addresses in the country to which they are registered.

A second source of potential bias is that interconnection agreements are not perfect measures of data flows. These agreements imply that data can flow between two ASes, but not that data is flowing between the ASes. However, these agreements are highly correlated with self-reported traffic volume by ASes (Lodhi, Larson, Dhamdhere, Dovrolis and claffy, 2014). However, these interconnection agreements do not all result in the same level of exchange. The following discussion of the data is in Zhuo et al. (2020).

> First, we note that we are able to capture only part of networks activities the formation and termination of interconnection agreements, and the types of agreements. It is important to note that connectivity is not traffic, though there is evidence that IP address space advertised by BGP tables are strongly positively correlated with networks self-reported traffic volume for a large set of peer-to-peer interconnections (Lodhi et al., 2014). We do not know how much traffic exchange happens across an interconnection or how that traffc has changed over time. If major changes in traffic occurred purely through existing interconnections, causing increased or decreased investment in Internet infrastructure, it would be invisible in our data.

3 Fixed Costs of Interconnection

One significant fixed costs for internet exchange is fiber-optic cables that carry data across long distances. To account for this potential bias I collect data on submarine and terrestrial cable networks. For data on current submarine cables I use information from Telegeography,[4] and for data on unused, or "dark" cables I use data from the Submarine Cable Almanac, which began in 2011.[5] Each cable contains information about the set of physical landing points where the cable connects to terrestrial networks, which I project into a adjacency matrix of countries.

[4] TeleGeography. "Submarine Cable Map." Submarine Cable Map. https://www.submarinecablemap.com/.

[5] Submarine Telcoms Forum. "Submarine Cable Almanac." https://subtelforum.com/products/submarine-cable-almanac/.

Table 1: Terrestrial Cable Networks

Cable Network	Countries
TEA Cable	SE, FI, RU, CN, JP, HK, DE, UA, FR, NL, SE
TTK Eurasia	CN, MN, JP, FI, EE, LT, LV, PL, RU, NL
European Backbone	BE, BG, CZ, DK, DE, EE, IE, ES, FR, HR, IT, CY, LV, LT, LU, HU, MT, NL, AT, PL, PT, RO, SI, SK, FI, SE, BY, CH, GB, NO

However, multiple cables can meet in one landing point, which gives an opportunity to easily exchange data between the systems. This is another way of accounting for the fixed data exchange costs. For example, one country might pursue a cable with another to a landing point where data can then flow through the other cables that meet at that point. I create an adjacency matrix for cables with shared landing points, and use this to create another adjacency matrix of countries that can exchange data through one direct submarine path through two cables.

Furthermore, terrestrial cable networks allow countries to exchange data over ground. For this reason, all contiguous countries are also selected, since terrestrial fiber networks are not mapped and available the same way as submarine cables. I assume that if two countries are contiguous they do not have significant fixed costs to move data.[6] Finally, there are terrestrial networks that connect multiple countries. This is particularly important for European landlocked countries such as Switzerland and Austria, which are highly integrated into the global internet but do not have submarine cables. Russia also relies heavily on terrestrial cable networks to Europe and Asia.

I include three terrestrial fiber networks in the analysis, TTK Eurasia Highway, the TEA Cables, and the European fiber network. European networks include a variety of interconnected internet backbones including the Pan-European Crossing.[7] Countries in Europe have been highly interconnected since before the study period in 2008 (Rutherford, Gillespie and Richardson, 2004). TTK Eurasian highway has connected Europe and Asia through Russia since before the study period as well.[8] Additionally, Chinese and Russian operators have invested in the TEA Cable network to move data since 2010.[9]

I use this data to select dyads based on whether they had an existing fiber-optic cable route by the first month in the dataset (January, 2008). Controlling for fiber-optic cables after this date has the potential to introduce bias, since a trade agreement, military treaty, or conflict might influence whether a fiber-optic cable connects two countries in addition to whether internet service providers agree to exchange data.

[6] For example, see the International Telecommunications Union map of voluntarily disclosed terrestrial networks. https://www.itu.int/itu-d/tnd-map-public/

[7] "Global Crossing Expands Pan European Network; Secures Additional Rights of Way," March 9, 1999. https://www.fiberopticsonline.com/doc/global-crossing-expands-pan-european-network-0001.

[8] Totaltelecom. "TTK Triples International Data Transit Capacity between Europe and Asia," July 27, 2009. https://www.totaltele.com/447602/TTK-triples-international-data-transit-capacity-between-Europe-and-Asia.; Submarine Cable Networks. "ERA and HSCS Broaden the Eurasia Highway," July 15, 2011. https://www.submarinenetworks.com/systems/asia-europe-africa/hscs/era-hscs-eurasia-highway.

[9] "Rostelecom: Transit Europe-Asia The New Opportunities." Moscow, October 27, 2011. https://www.hkcolo.com/hkconnect/2011/event/thankyou/pdf/Rostelecom_Irina.pdf.

4 Treaties

Figures 1 and 2 contain the country-treaty observations where the status of the treaty changed between January 2008 and December 2018. It does not include all treaties - only treaties which were either entered into or withdrawn from during the study period. This data is taken from the *Alliance Treaty Obligations and Provisions Project (ATOP)* data on military agreements (Leeds et al., 2002). Version 5.0 of the dataset covers all alliances formed between 1815 and December 31, 2018. The treaties in Figure 1 contains treaties where the entry date was before 2012, and Figure 2 contains treaties with an entry date after 2012. The observations are labeled as the affected country, ATOP ID number, and phase of the alliance. Because one country may be joining a treaty with multiple existing members, one observation in either figure may affect multiple dyads. Treaty memberships that are active on the last day of 2019 are colored in red, while treaties that end before this are colored in blue.

Figure 1: New Treaties or Signatories (signed before 2012)

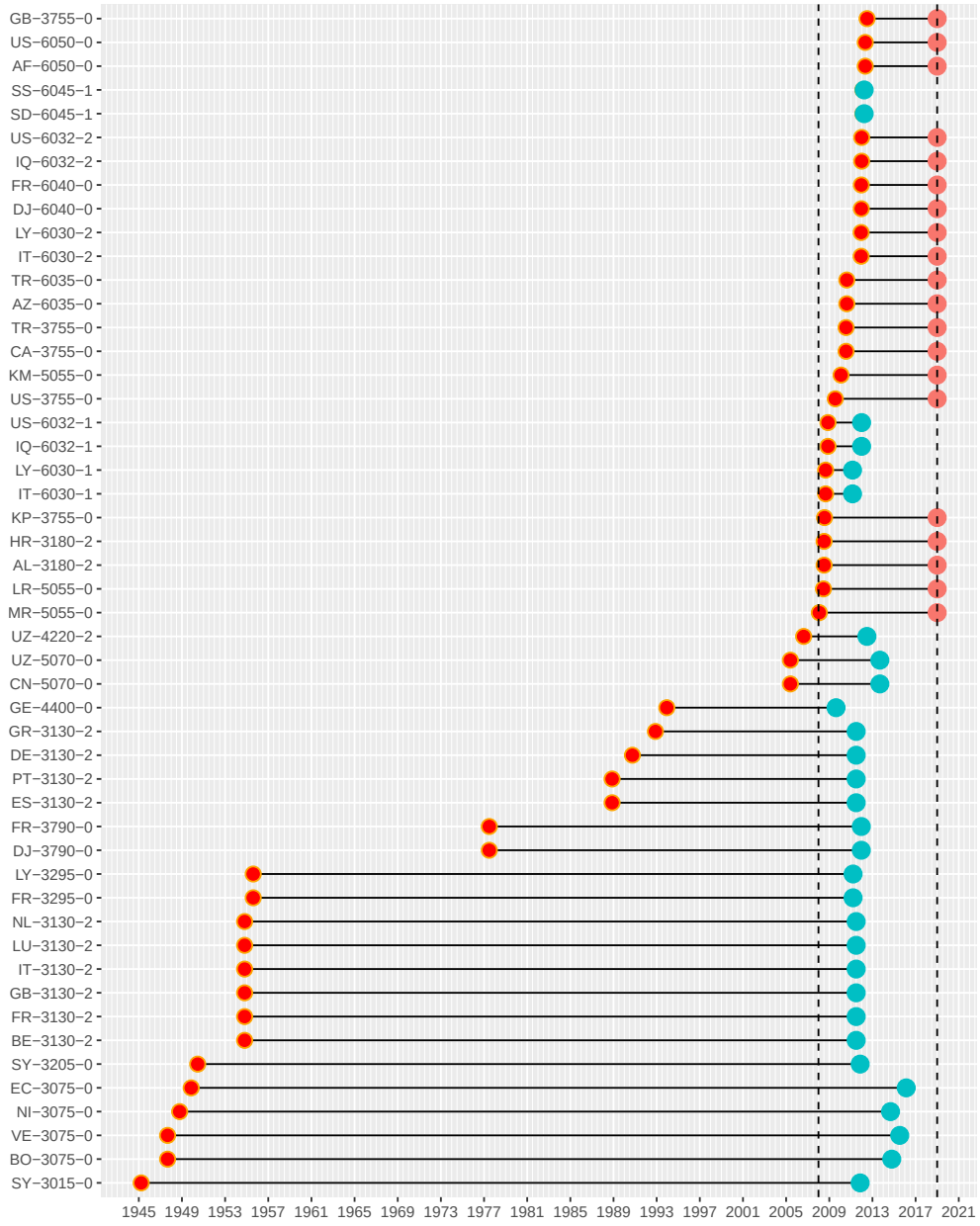
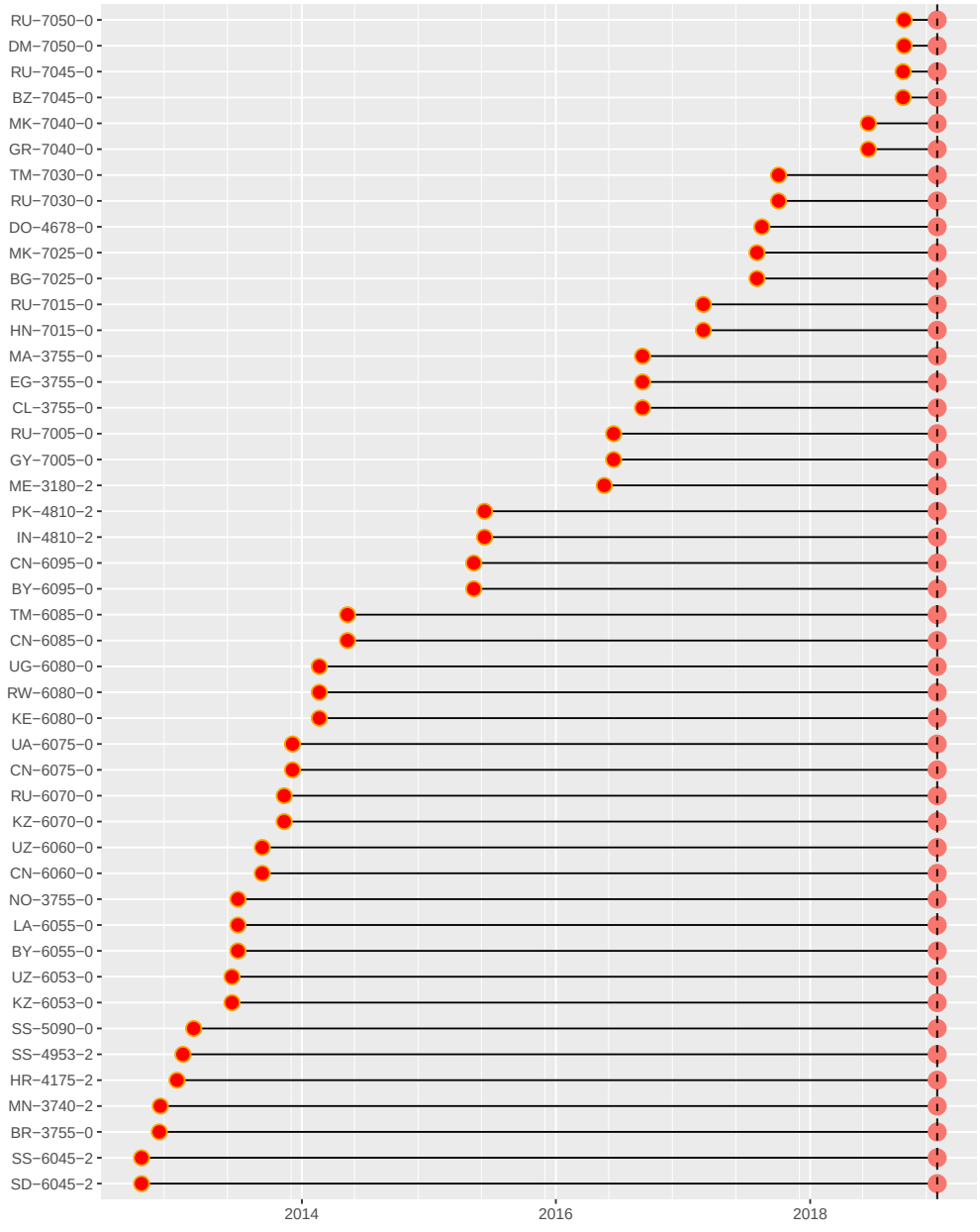


Figure 2: New Treaties or Signatories (signed after 2012)



5 Conflicts

MIDS This paper uses the Militarized Interstate Dispute (MIDs) Dataset "Dyadic MIDs 4.02". The dataset includes four categories of conflict - threat to use force, display of force, use of force, and insterstate war (Maoz et al., 2019). I consider cases where one state uses force, which MIDs considers as any case of border violation, blockage, occupation, seizure, clashes, raids, declarations of wars, or the use of chemical and biological weapons. This does not include cases of "display of force" such as fortifying borders, or "threat to use force." These conflicts are contained in Figures 3 and 4, which includes the affected dyad, the relevant MID #, and the dates that it was active.

Figure 3: Active MIDS 2006-2015 (January, 2006 through March, 2011)

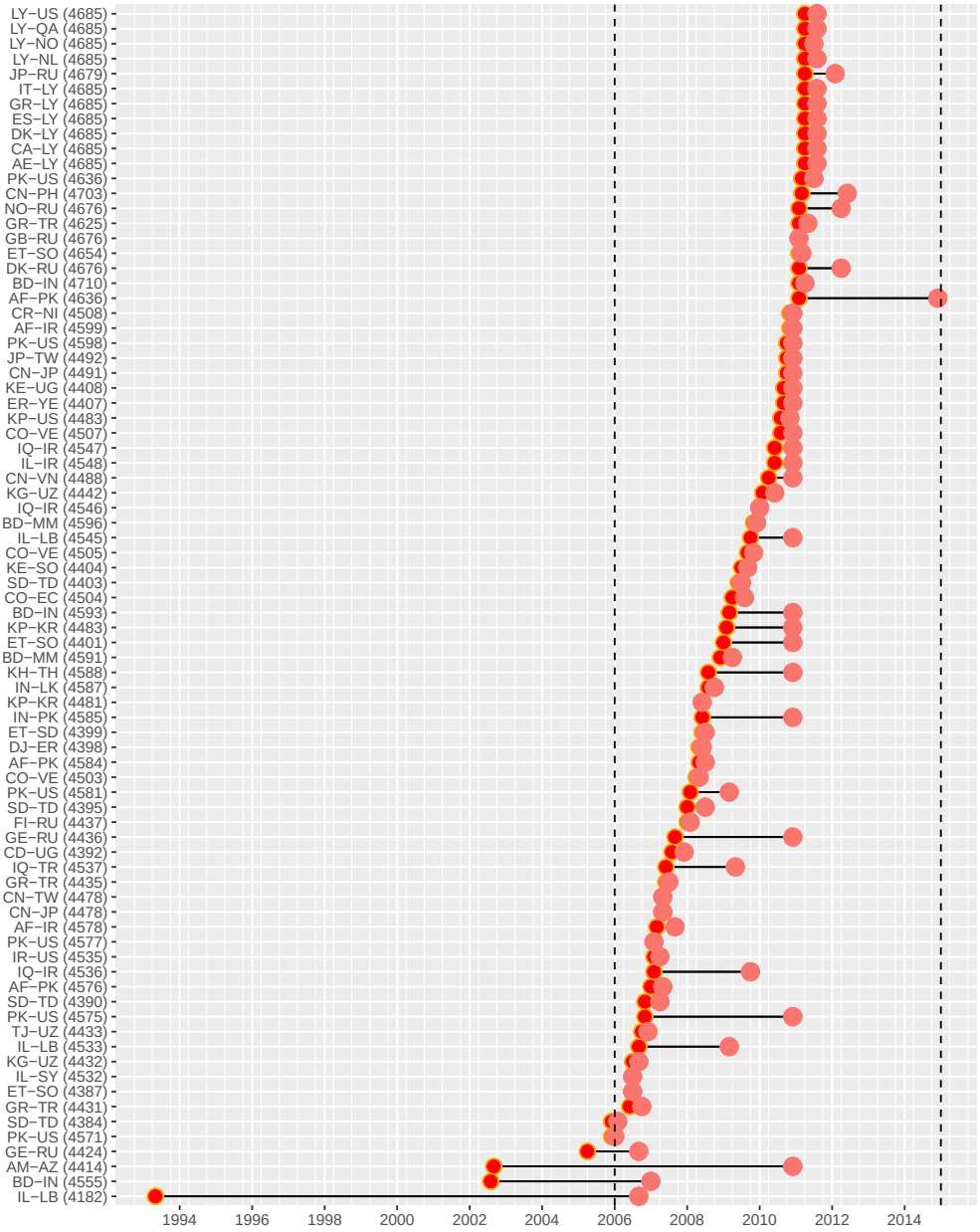
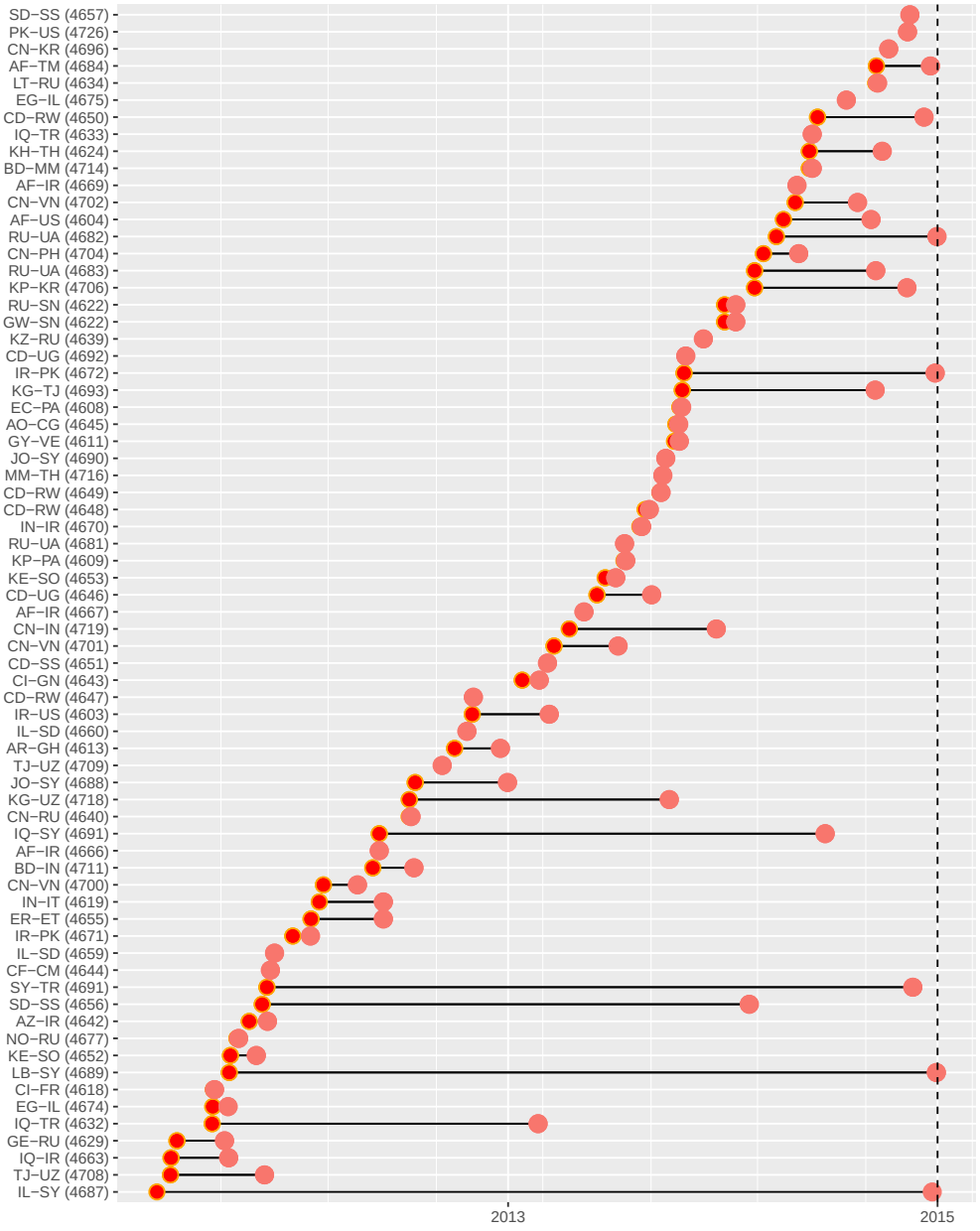


Figure 4: Active MIDS 2006-2015 (starting after March, 2011)



6 Results: Does Data Follow the Flag?

This section contains the main results in the paper with alternative approaches to modeling fixed effects and time. Table 2 contains the main results from the paper, and Table 3 contains these results for a sample of dyads with a submarine or large terrestrial cable link. These links are discussed in Appendix Section 3. Table 4 contains the results with fixed costs for each country in the dyad, rather than the dyad itself. To capture some of the fixed costs of interconnection within a dyad that do not change over time I include the logged distance between the two countries and an indicator

for whether they share a border. Table **??** models time as a series of non-linear spline terms, rather than as a intercept term, and contains fixed effects for the dyad. Finally, Table 6 contains the results with splines for time and fixed effects for the two countries in the dyad, along with logged distance and contiguity.

Table 2: Effects of Security Cooperation and Conflict on Interconnection

Dependent Variable:	**Provider-to-Customer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.185***	0.101	0.167***	0.173***
	(0.054)	(0.133)	(0.049)	(0.049)
Observations	374,544	374,328	591,840	591,552
Dependent Variable:	**Peer-to-Peer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.622***	-0.475***	0.441***	0.444***
	(0.087)	(0.156)	(0.153)	(0.153)
Observations	313,848	313,632	625,824	625,536
Fixed-effects				
Dyad	Yes	Yes	Yes	Yes
Month	Yes	Yes	Yes	Yes

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

Table 3: Effects of Security Cooperation and Conflict on Interconnection for Dyads Linked in 2006

Dependent Variable:	**Provider-to-Customer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.195***	0.093	0.185***	0.193***
	(0.057)	(0.138)	(0.051)	(0.051)
Observations	197,290	197,072	292,608	292,320
Dependent Variable:	**Peer-to-Peer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.623***	-0.523***	0.479***	0.482***
	(0.090)	(0.159)	(0.175)	(0.175)
Observations	166,552	166,334	275,904	275,616
Fixed-effects				
Dyad	Yes	Yes	Yes	Yes
Month	Yes	Yes	Yes	Yes

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

Table 4: Results with Alternative Fixed Effects

Dependent Variable:	**Provider-to-Customer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.980***	0.255	0.697***	0.693***
	(0.271)	(0.231)	(0.093)	(0.090)
log_distance	-0.978***	-1.00***	-0.783***	-0.808***
	(0.065)	(0.063)	(0.075)	(0.073)
contiguity	0.433***	0.296**	0.580***	0.425***
	(0.161)	(0.142)	(0.168)	(0.143)
Observations	2,012,256	2,030,670	2,722,464	2,722,176
Dependent Variable:	**Peer-to-Peer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	1.10***	-0.611***	0.440***	0.444***
	(0.195)	(0.193)	(0.087)	(0.087)
log_distance	-0.568***	-0.571***	-0.434***	-0.434***
	(0.057)	(0.057)	(0.053)	(0.053)
contiguity	0.158*	0.135	0.161*	0.136
	(0.092)	(0.092)	(0.087)	(0.086)
Observations	1,701,000	1,716,532	2,566,368	2,566,080
Fixed-effects				
CountryA	Yes	Yes	Yes	Yes
CountryB	Yes	Yes	Yes	Yes
Month	Yes	Yes	Yes	Yes

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

Table 5: Results with Time Splines

Dependent Variable:	**Provider-to-Customer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.246**	0.249*	0.156**	0.162***
	(0.082)	(0.101)	(0.049)	(0.048)
s1	0.662***	0.647***	0.795***	0.785***
	(0.057)	(0.056)	(0.049)	(0.048)
s2	2.27***	2.32***	1.63***	1.61***
	(0.222)	(0.221)	(0.071)	(0.070)
s3	2.01***	2.10***	1.14***	1.14***
	(0.329)	(0.323)	(0.044)	(0.044)
Observations	374,544	374,328	591,840	591,552

Dependent Variable:	**Peer-to-Peer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.102*	0.079*	0.442**	0.445**
	(0.043)	(0.038)	(0.152)	(0.152)
s1	1.70***	1.69***	1.65***	1.64***
	(0.121)	(0.120)	(0.066)	(0.066)
s2	2.53***	2.55***	2.72***	2.72***
	(0.335)	(0.334)	(0.127)	(0.127)
s3	1.80***	1.84***	2.11***	2.12***
	(0.459)	(0.458)	(0.112)	(0.113)
Observations	313,848	313,632	625,824	625,536
Fixed-effects				
Dyad	Yes	Yes	Yes	Yes
Month	Yes	Yes	Yes	Yes

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

Table 6: Results with Time Splines and Alternate Fixed Effects

Dependent Variable:	**Provider-to-Customer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.342	0.322	0.695***	0.690***
	(0.200)	(0.255)	(0.094)	(0.091)
log_distance	-0.980***	-1.00***	-0.784***	-0.809***
	(0.065)	(0.063)	(0.076)	(0.073)
contiguity	0.441**	0.295*	0.580***	0.424**
	(0.165)	(0.142)	(0.168)	(0.143)
s1	0.662***	0.649***	0.764***	0.754***
	(0.057)	(0.056)	(0.047)	(0.047)
s2	2.27***	2.30***	1.57***	1.55***
	(0.223)	(0.223)	(0.069)	(0.068)
s3	2.00***	2.07***	1.13***	1.13***
	(0.331)	(0.329)	(0.043)	(0.043)
Observations	2,012,256	2,012,040	2,722,464	2,722,176

Dependent Variable:	**Peer-to-Peer Agreements**			
Effect:	Conflict		Cooperation	
Sample:	All	No RU-UA	All	No RU-UA
Coefficient	0.230*	0.322	0.441***	0.690***
	(0.101)	(0.255)	(0.087)	(0.091)
log_distance	-0.569***	-1.00***	-0.434***	-0.809***
	(0.057)	(0.063)	(0.053)	(0.073)
contiguity	0.161	0.295*	0.161	0.424**
	(0.092)	(0.142)	(0.087)	(0.143)
s1	1.69***	0.649***	1.65***	0.754***
	(0.121)	(0.056)	(0.065)	(0.047)
s2	2.50***	2.30***	2.72***	1.55***
	(0.334)	(0.223)	(0.126)	(0.068)
s3	1.76***	2.07***	2.11***	1.13***
	(0.459)	(0.329)	(0.112)	(0.043)
Observations	1,701,000	2,012,040	2,566,368	2,722,176
Fixed-effects				
CountryA	Yes	Yes	Yes	Yes
CountryB	Yes	Yes	Yes	Yes

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

7 Robustness Checks

This section presents a robustness check for the main findings in the paper (also Appendix Table 2). I check for robustness by sequentially dropping individual countries from the analysis to understand when one country has the potential to change the results in the paper. This would demonstrate a particular problem if removing a country in an "untreated" group significantly changed the results of the analysis. The figures present the point estimate for the main effect along with a 95% confidence interval.

The positive and significant association between military treaties and both customer-to-provider and peer-to-peer interconnection remains when Treated Dyads are dropped sequentially (Figures 7-8).

Figure 5: Effect of MID Conflicts on Provider-to-Customer (Dropping Treated Dyads Sequentially)

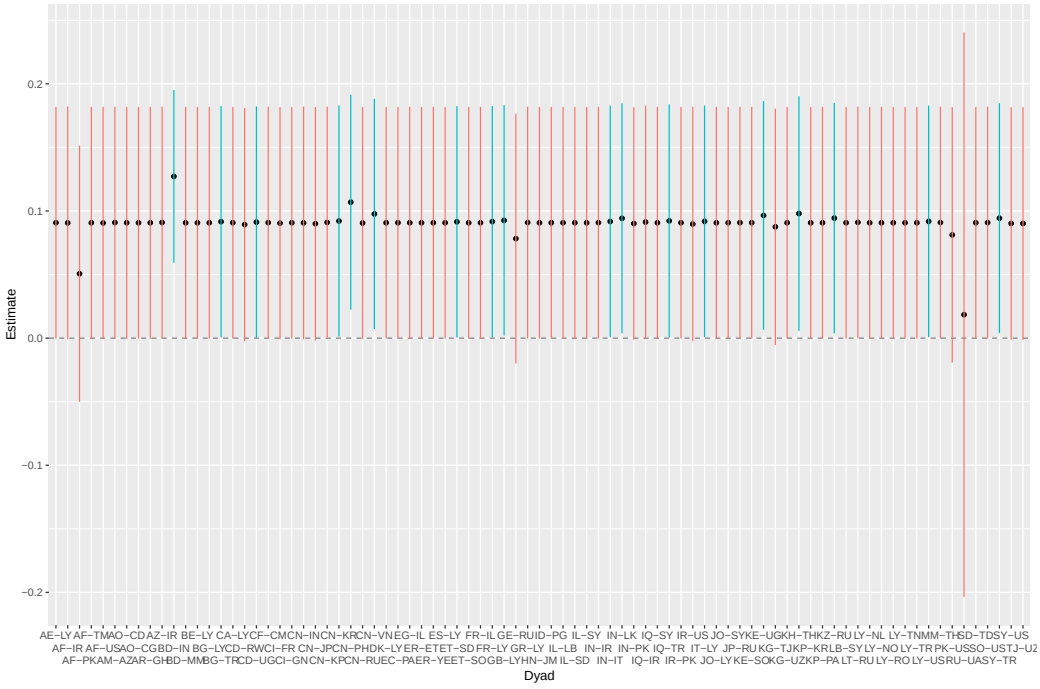


Figure 6: Effect of MID Conflicts on Peer-to-Peer (Dropping Treated Dyads Sequentially)

Figure 7: Effect of ATOP Treaties on Provider-to-Customer (Dropping Treated Dyads Sequentially)

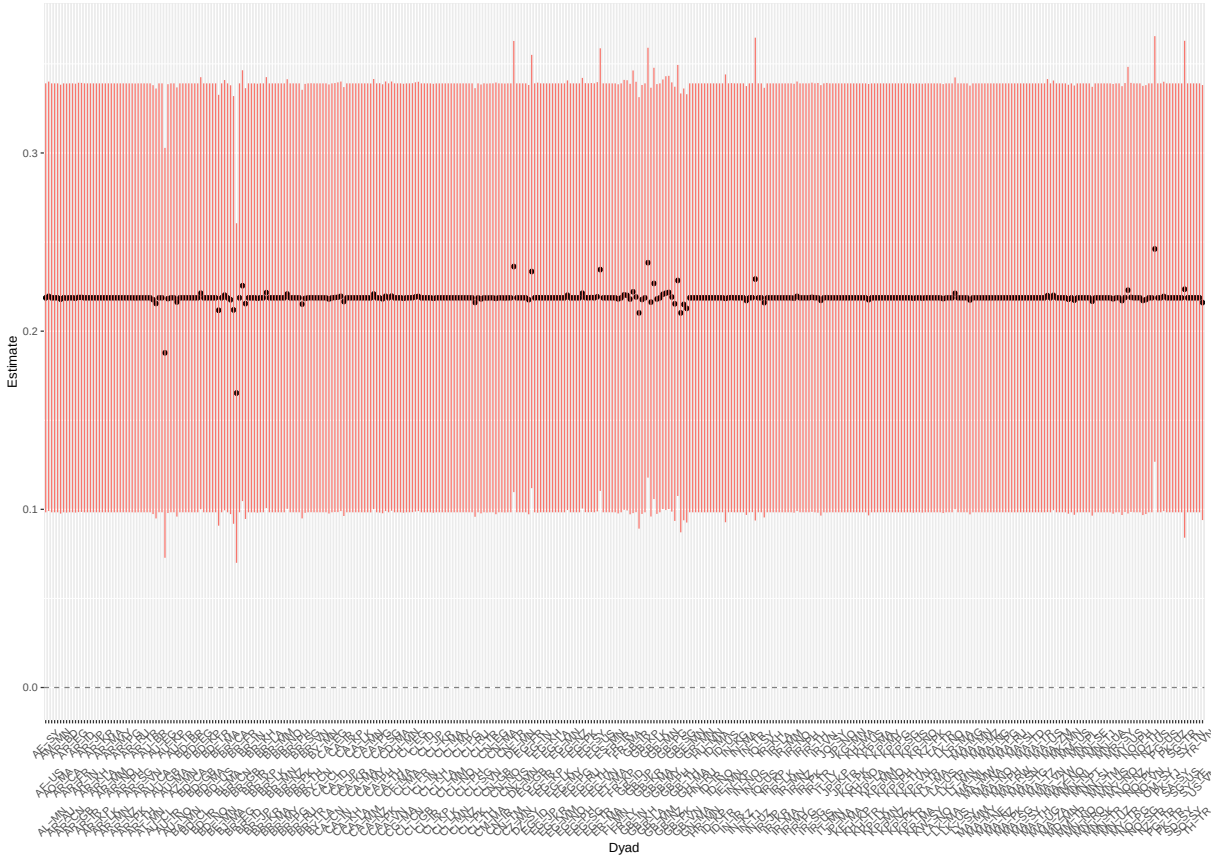
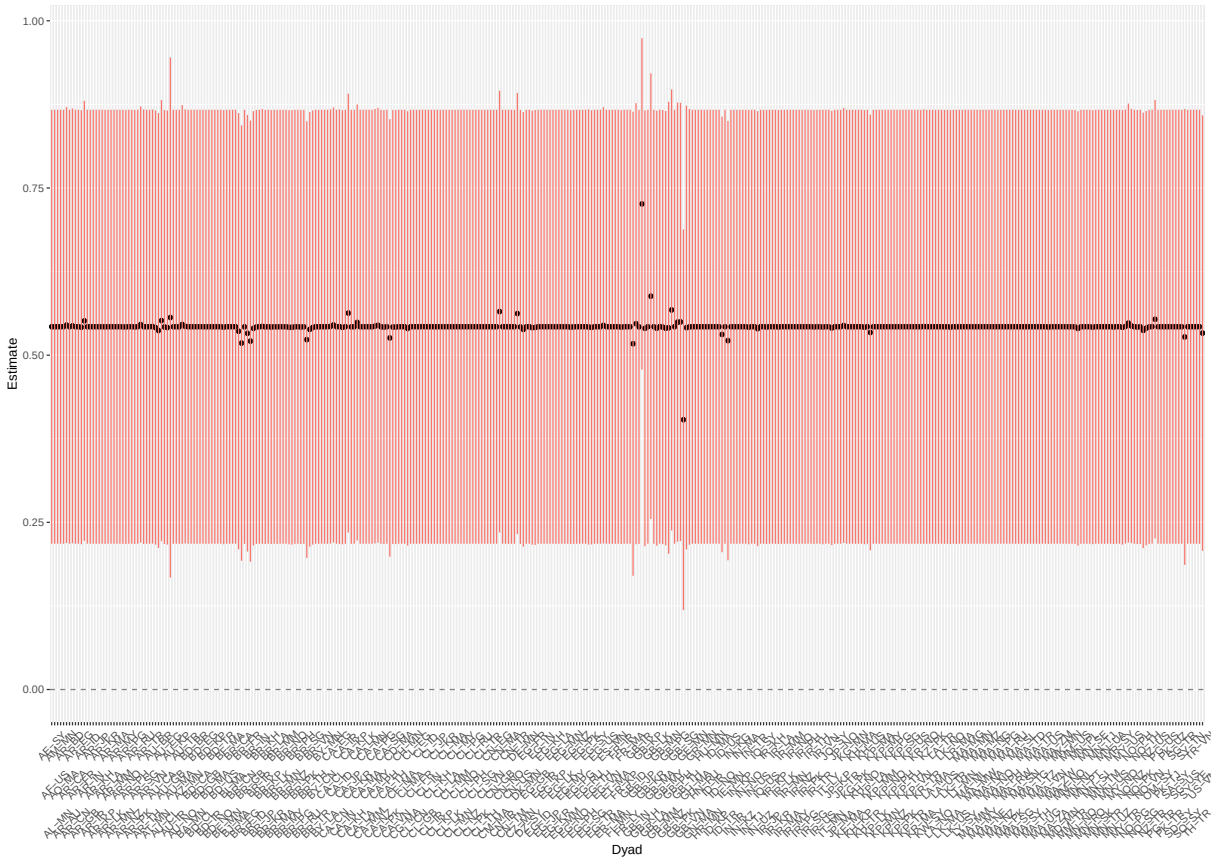


Figure 8: Effect of ATOP Treaties on Peer-to-Peer (Dropping Treated Dyads Sequentially)



References

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

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

Blum, Bernardo S. and Avi Goldfarb. 2006. "Does the Internet Defy the Law of Gravity?" *Journal of International Economics* 70(2):384–405.

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

Cowgill, Bo and Cosmina Dorobantu. 2014. "Worldwide Gravity in Online Commerce.".

Freund, Caroline and Diana Weinhold. 2002. "The Internet and International Trade in Services." *American Economic Review* 92(2):236–240.

Freund, Caroline L. and Diana Weinhold. 2004. "The Effect of the Internet on International Trade." *Journal of International Economics* 62(1):171–189.

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

Leeds, Brett Ashley, Jeffrey M. Ritter, Sara McLaughlin Mitchell and Andrew G. Long. 2002. "Alliance Treaty Obligations and Provisions, 1815-1944." *International Interactions* 28:237–260.

Lodhi, Aemen, Natalie Larson, Amogh Dhamdhere, Constantine Dovrolis and kc claffy. 2014. "Using peeringDB to Understand the Peering Ecosystem." *ACM SIGCOMM Computer Communication Review* 44(2):20–27.

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

Maoz, Zeev, Paul L. Johnson, Jasper Kaplan, Fiona Ogunkoya and Aaron Shreve. 2019. "The Dyadic Militarized Interstate Disputes (MIDs) Dataset Version 3.0: Logic, Characteristics, and Comparisons to Alternative Datasets." *Journal of Conflict Resolution* 6(3):811–835.

Rutherford, Jonathan, Andrew Gillespie and Ranald Richardson. 2004. "The Territoriality of Pan-European Telecommunications Backbone Networks." *Journal of Urban Technology* 11(3):1–34.

Zhuo, Ran, Bradley Huffaker, KC Claffy and Shane Greenstein. 2020. "The Impact of the General Data Protection Regulation on Internet Interconnection.".