British Journal of Political Science (2025), **55**, e93, 1–23
doi:10.1017/S0007123425000328

British Journal of
Political Science

ARTICLE

Digital Interdependence and Power Politics

Harry Oppenheimer

Jimmy and Rosalynn Carter School of Public Policy, Georgia Institute of Technology, Atlanta, GA, USA
Email: hoppenheimer@gatech.edu

(Received 4 October 2024; revised 14 January 2025; accepted 14 March 2025)

Abstract

This paper presents the first empirical analysis demonstrating how international security influences global data flows. Firms exchange data traffic to achieve fast, stable, and affordable access to digital infrastructure, driving digital interdependence. While international security shapes economic interdependence, the mechanisms linking the two – sanctions, tariffs, boycotts, and contracts – create little risk for Internet interconnection, which is commonly exempted from sanction and tariff regimes, not directly consumed by the public, and not enabled through traditional contracts. I theorize that international conflict generates cybersecurity externalities as state and non-state actors directly weaponize digital interdependence. Firms and their networks sit directly in the path of future conflicts. Leveraging network topographical measurements from computer engineering, I test whether conflict expectations increase states' mutual reliance to move data. I find robust evidence that power politics shapes digital interdependence and use additional analyses to argue that externalities, rather than state preferences, drive this process.

Keywords: interdependence; digital infrastructure; cybersecurity; international political economy; gravity models

Introduction

Firms trade in global markets, making states economically interdependent, but states make war and peace, shaping the partners with whom firms trade. Scholars have examined this dynamic since antiquity (Pollins 1989b). Today, digital interdependence shapes all parts of the global economy (Box and West 2016; High-level Panel on Digital Cooperation 2019; Weymouth 2023), yet we have a limited understanding of digital interdependence and power politics. National policies influence digital platforms (Goldsmith and Wu 2006; Roberts 2018) and domestic infrastructure (Gohdes 2015, 2024; O'Hara and Hall 2021), and central states benefit from an interdependent global Internet infrastructure (Farrell and Newman 2019). But, do states' security relationships shape how their firms route data outside their borders?

Just like economic interdependence, digital interdependence is created by firms agreeing to mutually beneficial exchange. In the Internet's case, firms operating networks exchange data traffic with others. Fifty thousand networks (owned by Internet service providers, universities, and businesses) in 190 countries provide Internet access to individual devices, and every network must connect with at least one other. Scaling this up, no country is an island on the Internet. Even North Korea relies on routes through China and Russia to connect with the web.

Digital interdependence – networks across borders moving data through one another – has substantial economic and security implications. Networks refusing to interconnect can make Internet access for entire continents more expensive, slower, and unstable (Chavula et al. 2017; Czernich et al. 2011). Networks' data routing decisions create asymmetric relationships

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

(Edmundson et al. 2018; Karlin et al. 2009), exposing states to spying and coercion (Clement and Obar 2015; Farrell and Newman 2019). Domestic censorship spreads through data routes, so digital interdependence means Internet filtering in Russia limits what users access throughout Central Asia (Ortwein et al. 2023).

Many authors address the 'trade follows the flag' theory of interdependence – beyond economic explanations such as factor endowments and comparative advantage, nations' security policies influence their trade (Anderton and Carter 2001; Gowa and Mansfield 1993; Long 2008; Mansfield and Bronson 1997; Polachek 1980; Pollins 1989a, Pollins, 1989b). The conventional wisdom and existing research on data routing focus on efficiency and cost, leaving little room for international security (Baake and Wichmann 1999; Economides et al. 2005; Greenstein 2020; Holme et al. 2008; Lodhi and Dovrolis 2010; Norton 2014). Authors diagnose barriers to international interconnection due to poor infrastructure (Rosa 2021), linguistic differences (Fanou et al. 2015), and regulatory regimes (Schumann and Kende 2013) – none have looked at how international security shapes the Internet's structure.

Power politics shapes economic interdependence because conflict creates risks for firms, and states have incentives to limit interdependence with adversaries. However, the feedback mechanisms underpinning the economic interdependence-security linkage, both top-down and bottom-up, translate poorly to digital interdependence and data traffic. Businesses fear conflict-related sanctions, and the low risk of sanctions between allies is one reason why firms prefer allied states' markets (Askari et al. 2003; Clark and Reed 2005; de Jonge Oudraat 2000; Mulder 2022). However, states frequently exempt Internet interconnection from sanctions regimes. Wars interfere with contract enforceability, undermining trade, but 99.5 per cent of interconnection agreements do not have contracts. Alliances and conflicts shape how and whether states enact tariffs (Baldwin 1985; Gowa 1994), but the WTO has placed a moratorium on tariffs for data flows for the past twenty-five years. The public boycotts products from adversaries (Heilmann 2016; Pollins 1989a; Trentmann 2019), yet Internet interconnection is a business-to-business service. Why should power politics and data routing align if the connections between the two are so tenuous?

Instead, this paper draws on computer science to explain the risk that interdependence presents to firms operating digital networks. Vulnerability to several exploits depends on who networks exchange data with, and networks often drop partners with poor cybersecurity practices. State and non-state actors alike leverage cyberspace to harm adversaries in response to worsening relations, including wars, diplomatic crises, and low-level conflicts. Firms and the networks they operate face significant risks from conflict externalities – they sit directly in the line of fire. In the economic interdependence literature, conflict expectations shape which firms trade with in peacetime (DiGiuseppe and Kleinberg 2019; Long 2008; Morrow 1999; Pollins 1989a, Pollins, 1989b). I theorize that firms align data routes with their conflict expectations to maintain stable access to global digital infrastructure.

My analysis leverages approaches from computer engineering, modelling routing between over 70,000 networks at the monthly level over eight years. This novel dataset charts relationships between Internet service providers across borders over time, providing new opportunities to understand how economic actors navigate risk in global markets. Alliances and formal treaties are associated with new agreements between networks, increasing digital interdependence between states. This result holds across different controls, robustness checks, and sensitivity analyses. Substantively, a treaty is associated with a 58 per cent increase in the number of agreements to route data directly between networks across borders.

An alternative to cybersecurity externalities is direct state intervention – states may encourage networks to route data through countries with which they have positive relations, or firms may fear government intervention during conflict, rather than cybersecurity risks. I carry out two analyses to test the limitations of a state-first story. States intervene in digital interdependence by strategically investing in digital infrastructure and submarine cables. I restrict my analysis to dyads

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

connected through physical infrastructure before the analysis, finding that conflict expectations continue to significantly impact networks' routing decisions. Furthermore, states effectively politicize trade through state ownership (Davis et al. 2019). State ownership is relatively common among Internet service providers, so we may expect state-owned networks to align more intensely with security policy. The effect of conflict expectations on digital interdependence limited to state-owned networks is indistinguishable from the global effect. Overall, the paper provides robust evidence that power politics influence the vast decentralized network shaping the global digital economy.

Why should we care about the relationship between digital interdependence and power politics? This paper updates and adapts our existing theories of economic interdependence to the digital age. It explains how states are interdependent through data flows and digital infrastructure, highlighting the private actors driving this phenomenon. We exist in an 'age of digital interdependence' as the Internet links societies in a way previously unimaginable (High-level Panel on Digital Cooperation 2019), yet we know little about the politics of this new world.

States have fewer mechanisms to control digital interdependence than economic interdependence and often attempt to depoliticize data routing. However, conflict generates cybersecurity risks, aligning the Internet's structure with conflict expectations. States do not need to directly influence digital interdependence, or even possess the capacity to do so, for the Internet to align with security policy. Firms and their networks directly experience the consequences of deteriorating interstate relations. Recognizing this dynamic deepens our understanding of the politics of interdependence (Cooper 1986; Deutsch 1954; Farrell and Newman 2019; Gartzke et al. 2001; Keohane and Nye 1977; Rosecrance and Stein 1973), digital infrastructure (Gohdes 2015, 2024; O'Hara and Hall 2021), and the effects of international security on the global economy and trade (Anderton and Carter 2001; Gowa and Mansfield 1993; Long 2008; Mansfield and Bronson 1997; Polachek 1980; Pollins 1989a, Pollins, 1989b).

Digital Interdependence

Interdependence is a defining feature of the international system (Deutsch 1954; Rosecrance and Stein 1973), generating policy coordination challenges (Cooper 1986), promoting or undermining stability (Gartzke et al. 2001), and providing states power to influence others (Farrell and Newman 2019; Keohane and Nye 1977). We know a lot about economic interdependence – what is digital interdependence?

Every Internet-connected device within two borders – one physical and one digital. For example, a reader may access this article in the USA and within a university's network. The Internet is not one network; it is an interdependent system of independent subnetworks called Autonomous Systems (ASes). These networks are operated by Internet service providers, universities, hosting companies, or digital service providers – any organization that wants to manage part of the Internet. The physical border is where the device is located on the map, and the digital border is the Internet subnetwork that services the device.

These networks need to connect with one another to reach devices in other networks – they cannot provide Internet access otherwise. ASes determine the routing rules within their networks – how data gets to each address within their borders. Individual network operators then negotiate routing relationships for how data enters and exits their borders. They directly exchange traffic either peer-to-peer (reciprocal and unpaid) or provider-to-customer (reciprocal and paid). Due to traffic ratios, networks peer when they are a similar size and pay when one network is larger (D'Ignazio and Giovannetti 2009; Economides et al. 2005; Huston 1998). In both cases, networks carry data for one another, and data flows directly between the two networks.

A useful analogy for Internet networking is a mail system. An AS is like a post office, and a computer is like an individual with an address. Address ZIP codes indicate which post office

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

delivers the mail to the front door. Governments determine how mail transits between post offices, but post offices create local routes to deliver mail to mailboxes. Local post offices do not need to know anything about outgoing mail other than the identity of the other post office that services the address. Large organizations (office buildings, universities, corporations) effectively have their own post office – the government post office does not deliver each letter to each individual. The post office delivers all mail to one address, and the mail room delivers it to the final destination. In the mail system, the government determines how networks connect – on the Internet, the networks negotiate these rules themselves.

Just like firm-level decisions scale up to economic interdependence, individual routing decisions scale up to digital interdependence – how data enters and exits a country's borders to reach global addresses. For example, Edmundson et al. (2018) found that, to access popular websites, 72 per cent of Indian and 84 per cent of Brazilian user data traversed through the USA, and 33 per cent of Kenyan access was routed through Mauritius. The routes determine this dependence – networks in Brazil rely on routes through US networks, and networks in Kenya rely on routes through Mauritius.

Just as forgoing trade drags a nation's economy, forgoing digital interdependence creates Internet infrastructure inefficiencies, increasing prices and reducing speeds (Box and West 2016; Chavula et al. 2017). For example, 66.8 per cent of intra-African Internet traffic has to leave the continent because of low interdependence between African networks (Gupta et al. 2014). Networks refusing interconnection can impact entire regions. Most famously, US-based Cogent and Sweden-based Telia, among the largest networks in their respective regions, stopped exchanging traffic in March 2008. Without direct pathways for data, large portions of the Scandinavian and the US Internet could not reach one another, effectively 'partitioning the Internet'.[1] Even with other paths, links between Cogent and Telia customers became slower and more expensive. Independent networks determine where, how, and when data moves into and out of their networks, scaling up to the structure of global data flows.

Efficiency and the Internet's Structure

Research on interdependence and power politics begins with purely economic and structural models, such as the gravity model of trade (Gowa 1994, 43; Keshk et al. 2004, 1160; Long 2008, 83; Polachek 1980, 60; Pollins 1989b, 468; Savage and Deutsch 1960, 552). States are interdependent because trade provides efficiency through comparative advantage, and they tend to become more interdependent with states that are geographically close or have complementary product profiles (Linnemann 1966; Tinbergen 1962).

The baseline equivalent for data exchange is that networks seek speed and stability within their price constraints (Holme et al. 2008; Lodhi and Dovrolis 2010; Marcos et al. 2020). Networks choose partners depending on their size (how much data they need to send), transit demands (where their data needs to go), potential partners' sizes (how much data they can receive), and infrastructural limits (where they can exchange data) (Economides et al. 2005; Greenstein 2020; Norton 2014; Weller and Woodcock 2013). Barriers exist due to structural constraints familiar to the non-digital economy – insufficient infrastructure (Rosa 2021), linguistic differences (Fanou et al. 2015), or mismatched licensing regimes (Schumann and Kende 2013).

The Internet's design prioritizes individual network decisions over central planning, and routing rules are self-organizing and highly decentralized (Feamster et al. 2004; Hall et al. 2011). In most countries, firms negotiate data routes without a regulatory backstop, and policymakers worldwide refrained from interfering in data routing decisions while passing rules on technical issues like net neutrality (Besen and Israel 2013; Clark et al. 2011; Singer 2014). Meier-Hahn

[1] Singel, Ryan. 'ISP Quarrel Partitions Internet'. *Wired*, 18 March 2008, available at https://www.wired.com/2008/03/isp-quarrel-par/.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

(2016) surveys global Internet regulations, finding that 'There is no central feature of the Internet that has been subject to as little formal regulation as Internet interconnection'. This is a distinct feature of the Internet's structure. In the USA, for instance, traffic exchange between telephone companies was always regulated, but regulators quickly found that their usual methods of understanding market size and scope did not translate to Internet interconnection (Maida 2013). Both economic and digital interdependence reflect an underlying efficiency – the question is then how power politics shapes firms' behaviours.

Economic Interdependence and Power Politics

Why do we need a new explanation for why power politics shape digital interdependence? After all, there is robust evidence that power politics shapes *economic interdependence*. The literature proposes four mechanisms linking power politics to firms' behaviours – sanctions, tariffs, boycotts, and contracts. Wars and disputes create risks through these channels (Anderton and Carter 2001; Gowa and Mansfield 1993; Mansfield and Bronson 1997; Polachek 1980). Alliances and formal treaties reduce the likelihood of conflict between signatories (Bearce et al. 2006; Leeds 2003; Long et al. 2007; Mattes and Vonnahme 2010; Owsiak and Frazier 2014), promoting bilateral trade by reducing conflict-related risks (DiGiuseppe and Kleinberg 2019; Long 2008; Morrow 1999; Pollins 1989b). States are also encouraged to reduce tariffs on allied states due to positive externalities (Gowa 1989). Yet, none of the existing mechanisms fit data flows as closely as traditional trade, and states make deliberate attempts not to politicize digital interdependence during conflicts.

Sanctions

Sanctions are the primary way states restrict firms from trading (Jentleson 2022). While sanctions occur outside of conflict to achieve political change through non-violent means, they are also explicit complements to war and accompany military disputes (Clark and Reed 2005; Mulder 2022). Many well-known sanctions began after states became militarily hostile, including UK sanctions during the Falklands War and US sanctions against Iran in 1979. Conflict reduces trade because states force firms to comply with sanctions, and alliances promote trade because they reduce the risk of conflict-related sanctions. Importantly, sanctions have to be clear and credible for firms to comply with them since non-compliance creates significant revenues (Morgan and Bapat 2003).

However, states commonly exempt interconnection agreements from sanctions. The US Office of Foreign Asset Control (OFAC) amended the Cuban Assets Control Regulations (CACR) in 2009 to address telecommunications, enabling companies to connect with Cuban providers.[2] In 2010, OFAC added language to the Sudan and Iranian asset control regulations to 'enable personal communications over the Internet'.[3] OFAC issued general license §515.542 in 2015, explicitly allowing US companies to peer with ETECSA, the Cuban state-run telecommunications provider, which continues to today.[4] This license also covers transactions (including payments in US dollars) for establishing connections with ETECSA, such as fibre-optic cable and satellite facilities. In 2024, ETECSA exchanges data with networks in the US, France, and Italy. Networks in other heavily sanctioned states, including Syrian Telecom and CANTV Venezuela, openly

[2] Cuban Assets Control Regulations, 31 CFR Part 515 F.R. § (2009).

[3] Cuban Assets Control Regulations; Sudanese Sanctions Regulations; Iranian Transactions Regulations, 75 FR 10997 (10 March 2010).

[4] US Department of the Treasury, Office of Foreign Assets Control, 'IS "peering" - an arrangement of traffic exchange between internet networks - authorized by the CACR?' FAQ 786, 6 September 2019, available at https://ofac.treasury.gov/faqs/786.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

exchange data traffic.[5] The EU Council clarified its Russia sanctions in June 2022, ensuring that sanctions 'do not apply to funds or economic resources that are strictly necessary for the provision of electronic communications services by Union telecommunication operators'.[6] Furthermore, many agreements are peer-to-peer, with no financial exchange, and there are no known cases where a government-sanctioned unpaid data exchange.[7]

Tariffs

While the economic statecraft literature focuses on sanctions, states also use tariffs to align firms with security policy (Baldwin 1985, 50; Gowa 1994, Ch. 4; Polachek 1980, 60). China placed an anti-dumping tariff on Australian wine and barley in 2020 after Australian Prime Minister Scott Morrison called for 'an objective, independent assessment' of how the COVID-19 pandemic began.[8] In 2019, India revoked Pakistan's most-favoured-nation status after the Pulwama attack that killed over forty members of the Indian Central Reserve Police Force, raising prices for Pakistani goods.[9] States gain security benefits from allies' economic growth and use tariffs to shape trade with this in mind (Gowa 1994).

However, data flows and interconnection agreements are not subject to tariffs. The Information Technology Agreement, adopted after the Uruguay Round in 1996, significantly restricts tariffs on several parts of the digital economy (Burri 2017). In 1998, the WTO's Second Ministerial Conference announced the Global Declaration on E-Commerce, which placed a moratorium on customs duties for electronic transmissions.[10] This moratorium is currently set to continue until at least 2026. States cannot align firms with security policy by placing tariffs on data routes to adversaries or lowering tariffs on data routes to allies. Again, states lack a key policy lever.

Boycotts

In addition to government intervention, consumer preferences and boycotts drive the trade-power politics relationship from the bottom up. This is the logic behind economic nationalism – conflicts reduce consumer demand for goods and services from adversarial nations. Importers experience a drop in demand and adjust their purchasing to non-boycotted countries to preserve market share (Heilmann 2016; Trentmann 2019). This can occur without an official government policy prohibiting purchases from the other state. As Pollins (1989a) notes, boycotts are most plausible as a mechanism when consumers can identify products by their country of origin and less plausible in intermediate goods where consumers have fewer opportunities to discriminate (p. 740).

However, interconnection is a business-to-business transaction. The public (Internet-consuming businesses and individuals) does not directly purchase data exchange agreements. The public purchases Internet access from the networks, which then interconnect with one another and drive digital interdependence. Consumer boycotts are a bottom-up mechanism

[5] https://bgp.he.net/AS11960#_peers, https://bgp.he.net/AS29386#_whois, https://bgp.he.net/AS8048#_peers.

[6] Council Regulation (EU) 2022/880 of 3 June 2022 amending Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, *Official Journal of the European Union* L 153/75.

[7] The initial TikTok/WeChat ban is the only case where sanctions included unpaid peering. However, this peering ban was never implemented. Subsequent discussions of banning TikTok and WeChat have not included proposals on prohibiting peering or interconnection with Tencent (the parent company of WeChat) or TikTok. In 2024, Tencent maintains a US peering presence in Seattle, Ashburn, and San Jose (https://www.peeringdb.com/asn/132203). Tencent exchanges traffic with large US networks, including Cogent, Level 3, and GTT Communications (https://bgp.he.net/AS132203#_peers).

[8] Westcott B. 'Australia Angered China by Calling for a Coronavirus Investigation. Now Beijing is Targeting its Exports'. *CNN*, 27 May 2020.

[9] Suneja K. 'Pakistan's Most-Favoured Nation Status Scrapped'. *The Economic Times*, 16 February 2019.

[10] Bond DE, Eglin R, Sabitha NR and Saccomanno I. 'WTO Extends E-Commerce Tariff Moratorium as Broader Negotiations Continue.' White & Case LLP. Our Thinking (blog), 7 March 2024.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

shifting the demand curve for products or services from adversarial states. For boycott risks to explain the digital interdependence-power politics relationship, consumers would need to both (1) know how their provider routes their data and (2) switch to a provider with different routing behaviours. Neither of these assumptions is plausible.

Contracts

Firms rely on contract enforceability to prevent cheating and settle disputes (Dixit 2003). Authors have noted for over a hundred years that wars interfere with contracts between firms through *force majeure* (Hall 1918) and expropriation (Harris 1961). Long (2008) argues firms rely on allied markets because 'As the institutional mechanisms for enforcing contracts or arranging compensation when a contract is broken become unreliable, firms will attain no recompense for breaches of contract by a trade partner' (p. 86).

However, 99.5 per cent of agreements between networks are 'handshake agreements' without formal or written contracts (Marcos et al. 2020; Weller and Woodcock 2013; Woodcock and Frigino 2021).[11] Agreements do not rely on states enforcing contracts or the threat of legal repercussions. Interconnection either benefits both networks or, when paid, can be withdrawn by either party. If agreements do not rely on mutually enforceable contracts in the first place, then there is no risk from disruptions in enforceability, and the promise of stable contracts with firms in allied states would not push firms to negotiate new agreements.

Power Politics and the Internet's Structure

Why should international security shape digital interdependence? States sign treaties and make alliance commitments, shaping firms' expectations of future conflicts. Rather than the risk of direct intervention, the prospect of conflict brings significant cybersecurity externalities. Over the past two decades, both state and non-state actors have leveraged cyberspace during wars, smaller military disputes, and diplomatic crises. Computer scientists have demonstrated that cybersecurity risks spread through networks' routing decisions – interdependent networks are mutually vulnerable to attacks. This dynamic shapes how networks interconnect outside of conflict. This is different from the weaponized interdependence literature, which focuses on how states work with domestic firms to monitor global data flows from a central position (Farrell and Newman 2019). Instead, interdependence is weaponized as data routes carry attacks, and firms' networks are directly disrupted. Alliances and treaties, by reducing conflict and cybersecurity risk expectations, increase the interdependence between two states' Internet spaces.

Treaties and Alliances Shape Conflict Expectations

Alliances help states manage competition and avoid war (Bearce et al. 2006; Leeds 2003; Owsiak and Frazier 2014), and they are viewed by the international community as a credible signal of two states' intentions to cooperate (Morrow 1994; Smith 1995, 1998). States even use alliances to manage relationships with potential enemies and reduce the likelihood of conflict (Weitsman 2004) or apply pressure to allies to maintain restraint against third parties (Pressman 2012). Treaties do not have to contain full alliances with defensive commitments to shape conflict expectations. Non-aggression pacts without concrete defensive obligations reduce the likelihood of conflict between signatories (Long et al. 2007; Lupu and Poast 2016; Mattes and Vonnahme 2010; Warren 2016).

[11] Hannigan M and Snijders J. 'Interconnection Agreements at Scale: Secret or Simple?' APNIC Blog (blog), 26 October 2017, available at https://blog.apnic.net/2017/10/26/interconnection-agreements-scale-secret-simple/.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Firms' choices on how to route data are determined by their desire for speed and reliability (Holme et al. 2008; Lodhi and Dovrolis 2010; Marcos et al. 2020). Firms' choices about who to trade with are motivated by a desire to maintain market share and profits, not only at the current moment, but into the future. This is why firms' conflict expectations, and not only conflict itself, influence trade (Long 2008). As Pollins (1989b) points out, 'a buyer could choose a seller from a friendly nation in order to minimize the possibility of economic disruption' (p. 741). Firms negotiating data routes must do the same – manage risk among their existing partners to ensure stability and speed while minimizing potential disruptions. The concern in this case is identifying the risk from connections to countries that may be future adversaries. Drawing on computer engineering, I explain that interdependence creates vulnerability to cyberattacks and externalities, and the prospect of future conflicts increases the potential for cyberattacks from both state and non-state actors. Firms' networks rapidly become part of escalating interstate conflicts.

Conflicts Create Cybersecurity Risks

Worsening relations increase the risk of cyberattacks across borders. The cybersecurity literature is sceptical that cyberattacks alter the balance of power or fundamentally change warfare (Gartzke 2013; Rid 2013; Valeriano and Maness 2015). However, cyberattacks, even if they do not change the course of wars, frequently accompany them (Kostyuk and Zhukov 2019). Wars and invasions often begin with cyberattacks. Russia launched distributed-denial-of-service (DDoS) attacks against Georgian and Ukrainian networks before land invasions in 2008, 2014, and 2022.[12] In 2016, the Australian Signals Directorate targeted Islamic State militants to assist the Iraqi Army with retaking Mosul.[13] While cyberattacks may not be decisive in conflict, they create significant disruptions for states in conflict.

Even if cyberattacks have a weak record of shaping war, experts still anticipate that wars increase cybersecurity risks. Former NSA Director Keith Alexander said in 2009 that 'If you think about it, phase zero of the next war, I think, is going to be in [the cyber domain]'.[14] 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'.[15] The 2023 US Department of Defense Cyber Strategy states, 'In the event of conflict, the PRC likely intends to launch destructive cyber attacks against the US Homeland'.[16] Actors believe wars create cybersecurity risks even if they have not materially changed war, and wartime attacks have economic consequences even if they do not shift the battlefield.

Militarized threats and disputes short of war increase the likelihood of cyberattacks. In 1999, the US National Infrastructure Protection Center issued an advisory noting 'multiple reports of hacking and cyber activity directed at US government computer networks, in response to the accidental bombing of the Chinese embassy in Belgrade' (Lin 2012). DDoS attacks, which are particularly damaging through interdependence, are commonplace during interstate disputes below the war threshold (Nazario 2009). China allegedly carried out DDoS attacks against the USA following a high-profile mid-air collision between US and Chinese military planes in 2001. In

[12] Przetachnik J and Tarpova P. 'Russia's War on Ukraine: Timeline of Cyberattacks'. European Parliamentary Research Service, June 2022; Danchev D. 'Georgia President's Web Site under DDoS Attack from Russian Hackers'. *ZDNET*, 22 July 2008, available at https://www.zdnet.com/article/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/.

[13] Probyn A. 'In the Heat of Battle, IS Militants' Phones Were Hijacked Thanks to Australians Inspired by Rick Astley'. ABC News, 4 June 2023, available at https://www.abc.net.au/news/2023-06-05/australian-cyber-spies-disrupted-islamic-state-militants/102425324.

[14] Lopez CT. 'Next War Will Begin in Cyberspace, Experts Predict'. www.army.mil, 27 February 2009, available at https://www.army.mil/article/17561/next_war_will_begin_in_cyberspace_experts_predict.

[15] Sanger DE and Barnes JE. 'US and Britain Help Ukraine Prepare for Potential Russian Cyberassault'. *New York Times*, 20 December 2021, sec. US.

[16] US Department of Defense. '2023 Cyber Strategy', 2023, p. 4.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

2007, Russia launched attacks against Estonian networks during a dispute over Soviet-era World War II memorials in Tallinn. Estonia blocked all international web traffic to mitigate the attack, effectively cutting all international interconnections. In 2019, the USA carried out cyberattacks on Iran in the wake of its drone attacks on Saudi Arabian oil facilities.[17] Security crises short of war create cybersecurity risks.

Cybersecurity risks occur alongside traditional risks arising from diplomatic disputes. As discussed earlier, China levied tariffs on Australia after Prime Minister Scott Morrison called for an investigation into the origins of COVID-19. In addition to tariffs, Australia observed a large spike in cyberattacks, which experts attributed to Chinese retaliation.[18] In 2024, Australia revealed that twenty Australian MPs belonging to the Inter-Parliamentary Alliance on China (IPAC) were targeted in the months after the diplomatic spat.[19] While dispute-related tariffs did not increase the cost of interconnection with China, the dispute increased cybersecurity risks from China.

Furthermore, even if states refrained from attacking one another through cyberspace during crises and disputes, their citizens often take matters into their own hands. This is linked to the 'rally around the flag' – individuals become more nationalistic and patriotic when their nation faces a threat from a foreign enemy (Mueller 1970; Parker 1995). This mechanism underpins the economic nationalist argument for the trade-interdependence relationship (Heilmann 2016; Michaels and Zhi 2010; Trentmann 2019). This is one of the unique aspects of conflict in the cyber domain – state and non-state actors interact in the same space. While the public does not directly consume data exchange agreements (and influence digital interdependence through the demand curve), they do have the opportunity to cause harm through digital interdependence.

Attacks from 'patriotic hackers' have targeted both government and non-governmental actors in adversarial states for at least twenty years (Denning 2001). Worsening relations between states prompt nationalist groups to target perceived enemies. In 2003, after Secretary of State Colin Powell addressed the Security Council, the US government issued a warning to American citizens carrying out attacks against Iraq.[20] Non-state hacker groups in India and Pakistan defaced public websites and carried out DDoS attacks after the 2008 Mumbai terrorist attacks and the 2016 Uri border clashes (Baezner 2018). Vietnamese and Chinese hackers defaced websites during the Spratly Islands dispute in 2011.[21] Russian-aligned group Killnet launched DDoS attacks against Lithuania in 2022 after Vilnius banned the transit of goods from Russia to Kaliningrad. In 2023, 'Anonymous Sudan' claimed responsibility for a DDoS attack against Microsoft in response to news of a potential US invasion. Even if states refrained from escalating conventional conflict and disputes into cyberspace, their citizens could disrupt their adversaries regardless.

Interdependence Transmits Cybersecurity Externalities

Cyberattacks move through the routes networks negotiate, wreaking havoc on a network's customers (Christin 2011). Networks do not want to directly exchange traffic with counterparts hosting malicious actors (Konte et al. 2015). Mustafa et al. (2022) found that the ability to handle malicious traffic was the most common interconnection requirement among the 1,295 US ASes.

[17] Ali I and Stewart P. 'Exclusive: US Carried out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials'. *Reuters*, 16 October 2019, sec. Cyber Risk.

[18] Tarabay J. 'How Hackers Hammered Australia After China Ties Turned Sour'. *Bloomberg.com*, 30 August 2021.

[19] Bourke LM. 'Aussie Spy Agencies Kept MPs in Dark after Chinese Hacking'. *The Nightly*, 5 May 2024, available at https://thenightly.com.au/politics/australia/spy-agencies-kept-australian-mps-in-dark-after-they-were-targeted-by-chinese-hackers-c-14531043.

[20] *BBC News*. 'US Hackers Told to Leave Iraq Alone'. 14 February 2003, available at http://news.bbc.co.uk/2/hi/technology/2760899.stm.

[21] *BBC News*. 'Vietnam and China Hackers Escalate Spratly Islands Row'. 9 June 2011, sec. Asia-Pacific, available at https://www.bbc.com/news/world-asia-pacific-13707921.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Meier-Hahn (2017) wrote for RIPE Labs (part of the non-profit Internet registry for Europe, the Middle East, and parts of Central Asia) that 'A network operator may legitimately shut down a peering session when his network receives malicious traffic (such as a DDoS attack) from its neighbours'. Cybersecurity company Cloudflare noted in a presentation to RIPE NCC that networks often de-peer partners that send significant attack traffic.[22] Dourado (2012) describes 'de-peering' as the 'ultimate enforcement mechanism' against insecure networks, allowing the Internet to promote security practices without formal rules (p. 9).

Networks publicly drop transit clients due to cybersecurity risks and malicious traffic. In 2008, journalists investigated Internet host McColo, which allowed cybercriminal gangs to operate without restrictions. McColo was responsible for 75 per cent of the daily spam emails in the USA and hosted the botnets Rustock, Srizbi, Pushdo/Cutwail, Ozdok/Mega-D, and Gheg.[23] Immediately after the report, Hurricane Electric and Global Crossing, two of the Internet's largest data transit networks, cut off McColo from their services. Global Crossing justified the decision based on the risk to their peers and customers.[24] The effects were profound – de-peering McColo immediately decreased global email spam by 70 per cent. Malicious ISP Atrivo was dropped by its providers the same year due to poor cybersecurity practices.[25] In 2022, two US-based Internet backbone companies – Cogent and Lumen – referenced cyberattacks when de-peering Russian clients. Cogent stated the company did not want its data transit routes to be 'used for outbound cyberattack or disinformation'.[26] Lumen explained to its Russian clients, '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'.[27] Interdependent networks generate significant risk for one another, and providing data transit for a network with significant outbound malicious activities has significant costs.

Networks 'de-peer' because malicious traffic interferes with their networks – they are either voluntarily carrying data with no direct benefit or providing data transit to a network that harms their other customers. By de-peering the target network forces traffic through other channels, delaying it or raising the cost for the malicious actor. Importantly, this occurs without direct state intervention or regulatory capacity – interdependence with a network sending malicious traffic creates a direct risk to the network's stability.

Distributed denial of service attacks (DDoS), where attackers overwhelm target networks through data traffic, are one prominent example where digital interdependence directly determines opportunities to exploit networks (Hui et al. 2017).[28] Returning to the mail system analogy, a DDoS attack would be one person sending a thousand letters to another. Faced with so much information, the recipient would have to slow down to identify the good information from the bad, or just stop reading their mail. Additionally, the post office has to deliver each letter, interfering with its ability to get mail to everyone else in the neighbourhood. The malicious mail is coming from another post office's address area, and it is easier to carry out attacks through nearby post offices.

[22] Levy MJ. 'DDoS Mitigation at CloudFlare'. Presented at the RIPE SEE4, Beograd, Serbia, 22 April 2015.

[23] Krebs B. 'Major Source of Online Scams and Spams Knocked Offline'. *Washington Post*, 11 November 2008.

[24] Krebs B. 'Internet Providers Cut off Host of Spam E-Mail'. *Los Angeles Times*, 13 November 2008.

[25] Hruska J. 'Bad Seed ISP Atrivo Cut off from Rest of the Internet'. Ars Technica, 23 September 2008.

[26] Timberg C, Zakrzewski C and Menn J. 'A New Iron Curtain Is Descending across Russia's Internet'. *Washington Post*, 4 April 2022.

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

[28] Prince M. 'The DDoS That Almost Broke the Internet'. The Cloudflare Blog, 27 March 2013, available at https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

These attacks are widespread and damaging – Zayo Bandwidth, a large telecommunications company, reported 103,000 DDoS attacks against its customers in 2023 alone.[29] The 'Slammer Worm' was one DDOS-based cyberattack that proliferated via data exchange agreements. In January 2003, the attack affected 75,000 hosts within ten minutes, shutting down Internet services in South Korea for hours and creating Internet outages in Thailand, Japan, Malaysia, the Philippines, and India.[30] The worm searched for nearby nodes to proliferate, overwhelming routers belonging to networks in adjacent networks. The networks directly exchanging data were the next ones targeted by the vulnerability (Moore et al. 2003).

To summarize, firms seeking stable, fast, and efficient access to global Internet resources exchange data traffic with counterparts across the Internet. These individual decisions scale up to digital interdependence – states' mutual reliance on accessing data across the Internet. Historically, international security shapes interdependence by forcing firms to manage risks from boycotts, sanctions, tariffs, and contracts. However, the public does not consume data exchange agreements, states are reluctant to sanction digital interdependence, data transmissions are exempt from tariffs, and these agreements do not rely on contracts. Despite this, international conflict and disputes increase cybersecurity risks due to both state and non-state activity. Interconnection creates cybersecurity vulnerability between networks, often influencing their data routing decisions. Firms, seeking to minimize the disruption from cyberattacks and maintain robust access to global data flows, should align their routing decisions with conflict expectations to minimize conflict-related cybersecurity risks.

Methods and Data

The analysis uses the gravity model, a common econometric tool in the study of trade, including studies on the effects of security on trade (Gowa 1994; Keshk et al. 2004). In the canonical model, imports between countries i and j are a function of the size of their economies and a transaction cost term. This cost is often measured as distance but can also be border walls, similarities in regulatory regimes, or rivalry. Instead of trade flows, I model the number of interconnection agreements between networks in two countries as a function of their bilateral security relationship. While the gravity model typically models imports from i to j, this analysis relies on the more general model of the total volume between i and j.

$$E(y_{ijt} \mid x_{itj}, \alpha_{it}, \gamma_{jt}, \eta_{ij}) = \lambda_{ijt} = \exp(x'_{ijt}\beta + \alpha_{it} + \gamma_{jt} + \eta_{ij})$$

In the above equation, the expected interdependence between networks in countries i and j in month t (y_{ijt}) is modelled through time-varying fixed effect α_{it} for country i and γ_{jt} for country j, where η_{ij} controls the time-invariant dyadic relationship between countries i and j.

This high-dimensional fixed effect approach is the 'three-way gravity model' common in the literature (Anderson 2011; Baldwin and Taglioni 2006; Baltagi et al. 2003; Baltagi et al. 2015; Carter and Poast 2020; Gowa and Hicks 2013; Weidner and Zylkin 2021; Yang and Zhang 2023). This specification controls for all time-variant country-level factors affecting Internet interconnection (infrastructure investment, country-specific business cycles, the number of Internet users), along with time-invariant dyadic factors affecting the two countries (distance, contiguous borders, shared language, colonial relationships). Following best practices, I use two-way clustering standard errors for the dyad and month (Aronow et al. 2015; Carlson et al. 2024). With this model in place, I measure the number of interconnection agreements between networks in a dyad in the period before and after a treaty, conditional on the fixed effects.

[29] Zayo Bandwidth. 'Protecting Your Business from Cyber Attacks: The State of DDoS Attacks', 2023.

[30] BBC News. 'Virus-like Attack Hits Web Traffic'. 25 January 2003.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Measuring Digital Interdependence

The Center for Applied Internet Data Analysis (CAIDA) gathers detailed Internet routing data. This paper leverages two CAIDA datasets, *AS Relationships* with agreements between networks (The CAIDA UCSD AS Relationships Dataset, 2010-2018, 2013), and *AS Organizations* mapping autonomous system numbers to organizations (The CAIDA UCSD Inferred AS to Organization Mapping Dataset, 2010-2018, 2014). CAIDA collects Internet routing data by working with partners to contact hosts and record how the Internet routes connections (Dimitropoulos et al. 2007; Dimitropoulos et al. 2005; Luckie et al. 2013). This data are monthly lists of networks directly exchanging data traffic.

To measure interdependence, I match AS numbers to states. However, AS ownership and location change over time. CAIDA publishes information about AS ownership using data from Internet registries dating to 2004 in four-month intervals. Each entry includes the autonomous system number, a self-reported country, organization identification, and some basic information about network owners. I combine the four-month snapshots of AS ownership into one dataset with owners of AS numbers for the entire period. I am primarily interested in where the network is operating rather than where the organization owning the network is registered or located. I compare the network IP delegation file (which says which IP addresses the AS routes to) to an IP geolocation dataset (which says where those IP address blocks are) to confirm the primary physical location of IP addresses for each AS.

I merge and clean the CAIDA datasets to construct the number of agreements between networks in two countries (i, j) in each month (t). I combine both peer-to-peer and customer-to-provider agreements in this analysis. There are several important reasons for this. All agreements, regardless of type, involve direct data exchange across networks. Cybersecurity externalities pass through agreements of either type – these agreements are, at the technical level, the same as part of the Border Gateway Protocol. We have no theoretical justification for why international security would affect one of these types of agreements but not the other. Furthermore, researchers at CAIDA know agreements exist but infer the type from each agreement's place in the larger network. There are also paid peering relationships in addition to unpaid peering relationships. We cannot be entirely confident whether the tag of provider-to-customer or peer-to-peer is correct, only that the two networks have a direct relationship. Certainly, the world of Internet measurement is more complex than I consider here. However, given the fixed effects specification, we can control for the number of networks in each country and other factors, isolating how dyad-level political factors affect the density of Internet interconnection between states' Internet spaces.

This data has limitations. While CAIDA has the most comprehensive Internet topography measurements dataset, there may be portions of the Internet space where CAIDA has less visibility. However, there is no reason to believe that a measurement error, such as missing agreements, is correlated with conflict expectations. The data source would be biased if CAIDA had less visibility or monitoring capabilities in countries signing treaties.[31] CAIDA does not provide information about data exchange prices, data flow capacity within agreements, or actual data flows. This data at scale has never been available for academic research and does not exist at the global level (Nguyen and Paczos 2020; Nicholson and McHenry 2016). An agreement indicates that data is flowing between two networks, and the absence of an agreement means that data is not flowing directly between two networks.

The measures in this paper improve significantly on previous measures of digital interdependence. Freund and Weinhold (2002) and Lopez Gonzalez and Ferencz (2018) measure interdependence by interacting with dyadic Internet penetration rates and IP-address space size. This indicates that countries depend on the Internet, but not that they are interdependent. Blum

[31] For more information on sources of bias in Internet measurement data, see Sermpezis (2022).

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

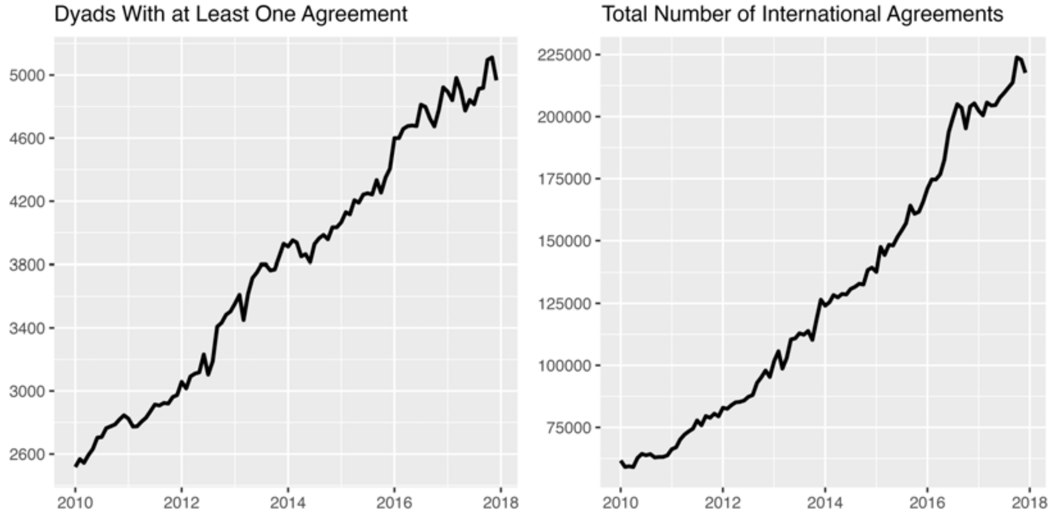

Figure 1. Trends in Digital Interdependence (January 2010–December 2017).

and Goldfarb (2006) and Cowgill and Dorobantu (2014) measure cross-border data flows through Google transaction patterns and click streams. However, this is platform-dependent – Google patterns differ from Facebook patterns, and platform usage varies widely cross-nationally. Data exchange remains a fundamental part of the Internet despite the rise of cloud platforms and content delivery networks (CDNs) because local providers must still get their data to local cache servers (Huston 2016; Kolkman et al. 2022). CAIDA's datasets are standard within the networking literature and have been used to understand the effects of data privacy laws on the Internet's structure in Europe (Zhuo et al. 2021).

There are 173 countries in this analysis, resulting in 29,070 unique directed dyads over ninety-six months from January 2010 through December 2017. In January 2010, there were 61,632 agreements between networks in these dyads. By December 2017, the number of agreements increased by 253.1 per cent to 217,618.[32] Figure 1 contains the number of dyads with at least one direct agreement and the total number of international agreements. In January 2010, 8.7 per cent of dyads had at least one connection. By December 2017, 17.1 per cent of dyads had at least one connection. This is a non-stationary process where cross-border agreements increase an average of 1.37 per cent per month.

Between 2010 and 2017, 21,730 of the 29,070 dyads never had a direct agreement. Among dyads with at least one agreement, 48.3 per cent of the individual observations are zero. This is a widely recognized challenge for gravity and fixed effects models. The gravity approach models logarithmic trade values, which are undefined for zero, and drops all zero values. There are significant drawbacks to adopting this approach for digital interdependence – both zero and changes from zero have substantive importance. In trade data, zeros are often assumed to be positive but undetectable flows. In digital interdependence, zero is a substantive value, indicating that no networks directly exchange traffic. A change from zero to one is critical since it indicates that data can directly flow between networks operating in the two Internet spaces.

I adopt Santos Silva and Tenreyro's (2006) solution, modelling raw agreement values as count data with a Poisson distribution. While Santos Silva and Tenreyro (2006) model continuous data, interconnection is measured as a count variable. The average number of dyadic connections is 4.39

[32] The technical collection process, the cleaning process, and potential biases in this data are discussed further in Appendix Section 1.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Table 1. Effects of Treaties on Digital Interdependence

	Dependent Variable			
	Internet Interconnection Agreements			
	(1)	(2)	(3)	(4)
Allied	0.4606*** (0.0839)	0.4615*** (0.0838)	0.4601*** (0.0839)	0.4610*** (0.0838)
Joint WTO		0.0221 (0.0447)		0.0226 (0.0447)
PTA			−0.0261 (0.0651)	−0.0274 (0.0651)
Observations	701,034	701,034	701,034	701,034

Model with Sender*Month, Receiver*Month, & Dyad Fixed Effects
Clustered (Dyad & Month) standard errors in parentheses
Signif. Codes: ***: 0.01, **: 0.05, *: 0.1

with a range between 0 and 4898 (BR-US in December 2017) and a standard deviation of 59.6. I account for this distribution and overdispersion with a quasipoisson approach.[33]

Alliances and Treaty Obligations

I use the *Alliance Treaty Obligations and Provisions Project (ATOP)* data on military agreements to measure conflict expectations (Leeds et al. 2002). Version 5.0 covers all agreements between 1815 and December 2018, containing 'formal agreements among independent states to cooperate militarily in the face of potential or realized military conflict'. This includes non-aggression pacts, but not arms sales or military aid agreements unless they include military cooperation obligations. Trade and alliances studies often use ATOP to identify treated dyads (Fordham 2010; Haim 2016). Between January 2010 and December 2017, 43 alliance entries into 30 unique treaties affected 640 directed dyads (2.2 per cent). I use the precise date each agreement was signed or when a new signatory entered into an agreement, and code all months after the new event as treated until the agreement ends. The appendix includes a plot containing the distribution of the treatment over time. There are new alliances affecting dyads distributed throughout the eight years in this analysis.

Other Covariates

The fixed effects specification in this design controls for the time-variant country effects and the time-invariant dyadic effects. However, I also control for potential time-variant dyadic covariates to minimize the potential that the effects of alliances are driven by another underlying positive change in states' political relationships. First, I control for joint WTO membership – during the study period, 11 countries joined the World Trade Organization. Second, I control for bilateral and multilateral trade agreements using the *Design of Trade Agreements (DESTA)* dataset Version 2.0 (Dür et al. 2014).

Data Follows the Flag

Table 1 reports the main results of the analysis. The first model does not include any other controls, but the fixed effects α_{it}, γ_{jt}, and η_{ij} capture many typical controls in other analyses. Models 2-4 include different variables capturing the evolving economic relationship across dyads.

[33] In the appendix, I replicate the main analyses with a linear modelling approach. The results do not change substantively from those contained in the main text.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

The results confirm the theory - conflict expectations significantly influence digital interdependence. Coefficients are from a quasipoisson model and substantively interpreted as $exp(\beta)$.

A treaty is associated with a 58.5 per cent increase in the number of agreements between networks in a dyad, and this effect is statistically significant at the 0.99 level. Models 2–4 add controls for states' economic relationships. The effect of treaties remains stable across these controls, with the coefficients ranging from 0.4601 to 0.4615. It also remains statistically robust at the 0.99 confidence level. In the appendix, I include a sensitivity analysis dropping treated dyads (with replacement), and this effect does not change substantively and remains statistically robust at the 0.00 confidence level.

State Preferences?

How can we rule out direct state intervention to increase digital interdependence with allies and align networks with security policy, or that the risk from conflict is due to preferences, rather than externalities? There are two ways that states might politicize digital interdependence directly – through investments in infrastructure and state ownership.

States can shape digital interdependence by investing in and interfering with digital infrastructure. For example, in 2017, Facebook and Google proposed investing $300 million to build a fibre-optic cable between Los Angeles and Hong Kong with twelve times the capacity of the existing infrastructure.[34] In June 2020, the Federal Communications Commission blocked the Chinese portion of the license over Justice Department concerns it would 'increase the share of US 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' (Office of Public Affairs 2020).

The effect of alliances on interdependence might be driven by firms' expectations about their state's future investments in digital infrastructure. I reduce this risk by restricting the analysis to dyads already linked through digital infrastructure before 2010. I measure this link in two ways. First, through fibre-optic cables, which carry approximately 99 per cent of transcontinental data traffic (Starosielski 2015). These cables are a related but distinct part of digital interdependence. Second, through Internet exchange points, where networks physically meet to exchange traffic.

I gather data on current submarine cables from Telegeography and data on unused or 'dark' cables from the Submarine Cable Almanac.[35] Countries are 'selected' if they are partners in a submarine cable meeting at a shared landing point. All contiguous countries are selected due to unmapped terrestrial fibre networks. I also include the three largest terrestrial fibre networks – the European Backbone, the TEA Cable, and the TKK Eurasia Highway.

Internet exchange point data comes from Packet Clearing House (PCH), an international organization that provides support for Internet infrastructure. The PCH 'IXP Directory' helps networks identify locations where they can exchange data. I collect this data and manually verify each starting date. In January 2010, there were 319 IXPs in eighty countries. Both of these infrastructures are necessary for the analysis. Without considering IXPs, one could assume landlocked European countries are digital islands, and without submarine cables, it would be unclear whether smaller island nations were connected to anyone. I detail how I collect both the cable and IXP data in Appendix Section 3.

I use this data to select dyads based on the first month (January 2010). I select dyads that are either connected through physical cables (or contiguous) or both have an Internet exchange point. This selection reduces the number of dyads by 67.6 per cent from 29,070 to 9,422. Additionally,

[34] Strohm C and Shields T. 'Justice Department Opposes Google's Undersea Cable From China'. *Bloomberg.com*, 28 August 2019; O'Keefe K, FitzGerald D and Page J. 'National Security Concerns Threaten Undersea Data Link Backed by Google, Facebook'. *Wall Street Journal*, 28 August 2019, sec. Politics.

[35] TeleGeography. 'Submarine Cable Map'. Submarine Cable Map; Submarine Telcoms Forum. 'Submarine Cable Almanac'.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Table 2. Effects of Treaties on Digital Interdependence for Dyads Linked in 2010

	Dependent Variable			
	Internet Interconnection Agreements			
	(1)	(2)	(3)	(4)
Allied	0.4532***	0.4541***	0.4522***	0.4531***
	(0.0846)	(0.0844)	(0.0845)	(0.0844)
Joint WTO		0.0202		0.0211
		(0.0460)		(0.0461)
PTA			−0.0471	−0.0489
			(0.0759)	(0.0758)
Observations	459,190	459,190	459,190	459,190

Model with Sender*Month, Receiver*Month, & Dyad Fixed Effects
Clustered (Dyad & Month) standard errors in parentheses
Signif. Codes: ***: 0.01, **: 0.05, *: 0.1

Table 3. Effects of Treaties on Digital Interdependence for State-Owned Networks

	Dependent Variable			
	Internet Interconnection Agreements			
	(1)	(2)	(3)	(4)
Allied	0.3950***	0.3950***	0.3951***	0.3952***
	(0.1031)	(0.1032)	(0.1032)	(0.1033)
Joint WTO		0.0014		0.0039
		(0.0582)		(0.0582)
PTA			0.0639	0.0642
			(0.0956)	(0.0958)
Observations	374,698	374,698	374,698	374,698

Model with Sender*Month, Receiver*Month, & Dyad Fixed Effects
Clustered (Dyad & Month) standard errors in parentheses
Signif. Codes: ***: 0.01, **: 0.05, *: 0.1

the percentage of dyads affected by changes in treaty status increases from 2.2 per cent to 4.7 per cent. The excluded dyads with the greatest digital interdependence are the UK-Zimbabwe and Bulgaria-USA. Table 2 contains the results for the main analysis, limited to dyads with fixed infrastructure costs in January 2010.

Similar to the unrestricted sample results in Table 1, the relationship between alliances and peer-to-peer data exchange remains positive and significant. The difference in the effects, controlling for existing infrastructure, is minuscule. The coefficient for the effects of alliances on digital interdependence is 0.0074 smaller. As a simple way of comparing these coefficients, we can conduct a Z test between the full analysis and the constrained analysis (Cohen et al. 2003).[36] For Model 1, the Z-score is 0.06, indicating that there is no statistically significant difference for the effect of conflict expectations on digital interdependence when limited to dyads connected through physical infrastructure. Future research can examine how states choose to invest or intervene in infrastructure to raise or lower the costs of interdependence with allies and adversaries.

Davis et al. (2019) demonstrate that states effectively politicize trade through state-owned enterprises. I restrict my analysis to networks operated by state-owned enterprises to examine whether the effect of conflict expectations is state-driven, rather than externality-driven. If states

[36] $Z = \frac{\beta_1 - \beta_2}{\sqrt{S(\beta_1)^2 + S(\beta_2)^2}}$.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

direct firms to exchange traffic through allies, or if firms anticipate that conflicts lead to direct state intervention, the effect of conflict expectations on interconnection should be greatest for state-owned networks and Internet service providers. Conversely, if cybersecurity risks and conflict externalities drive the relationship, we would expect no difference between the global effect and the effect restricted to state-owned networks.

Carisimo et al. (2021) identified 989 networks operated by 467 state-owned enterprises. State ownership is common – there is at least one network operated by a state-owned enterprise in 125 countries, with China and Russia leading the way. I use this data to create a new dependent variable – the number of agreements where a state-owned enterprise operates at least one of the networks.

Table 3 contains the effects of treaties on digital interdependence through networks operated by a state-owned enterprise. Similar to the analysis for all countries (Table 1) and all countries linked through existing infrastructure (Table 2), alliances and treaties have a positive and significant relationship to digital interdependence. A treaty is associated with a 48.4 per cent increase in the number of agreements between Internet service providers in two states. These effects are smaller than the results for interdependence across all networks. Carrying out the same basic Z test across the estimates, we get a Z-score of 0.49. There is no statistically significant difference in the effect of conflict expectations on digital interdependence due to state-owned enterprises and digital interdependence overall. We would have expected the effect to be stronger if the effect of international security on interdependence was due to state preferences rather than externalities and cybersecurity risk.

Contributions

Digital interdependence – countries' mutual reliance on moving data through the Internet – is not merely a symbolic element of globalization. Fast and stable international data flows are the backbone of the modern global economy (Weymouth 2023). Networks that forgo interdependence create inefficient infrastructures that undermine access for entire continents (Chavula et al. 2017; Czernich et al. 2011). Asymmetric interdependence creates opportunities for countries to spy and coerce others (Clement and Obar 2015; Edmundson et al. 2018; Farrell and Newman 2019). How data flows between countries has economic and security implications, yet we have a limited understanding of the politics of digital interdependence.

Power politics shape economic interdependence because of specific risks to firms. Firms seeking to maintain their market share and minimize risk prefer to engage in states where the likelihood of conflict is low (DiGiuseppe and Kleinberg 2019; Long 2008; Morrow 1999; Pollins 1989a, Pollins, 1989b). After all, states determine tariff regimes, driving up prices on goods from adversaries and lowering prices on goods from allies (Baldwin 1985; Gowa 1994; Polachek 1980). Sanctions restrict trade with adversaries during conflict, punishing domestic firms failing to comply (Clark and Reed 2005; Jentleson 2022; Mulder 2022). States may not force domestic firms to follow through with commitments they make to firms in warring states (Long 2008). Consumer preferences and boycotts undermine economic interdependence even without state intervention (Heilmann 2016; Trentmann 2019).

Firms operating digital networks must exchange data traffic to access the greater Internet. Their routing decisions reflect a need for stable, fast, and affordable access, just as firms trade in international markets to acquire goods and services cheaply and efficiently. States commonly exclude interconnection agreements from sanctions, international rules significantly restrict their ability to tariff them, agreements do not rely on traditional contracts, and they remain obscure to the public.

Yet, firms exchanging data traffic sit along the front line of potential international disputes. I developed a theory that clearly links international security and digital interdependence.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Worsening bilateral relations create cybersecurity externalities from both state and non-state actors. This includes states using cyberattacks to prepare ground invasions or respond to diplomatic provocation, and nationalistic groups lashing out at their adversaries through an available medium. Interdependence creates cybersecurity risks as attacks leverage data routes to launch and command attacks. Cybersecurity risks shape how networks exchange data and which partners they drop outside of conflict. Firms, seeking to maintain stable and secure Internet access for their customers, align their external data routes with conflict expectations.

This paper demonstrates how digital interdependence is different from traditional economic interdependence. States retain less direct control over the direction of data flows and digital interdependence than the traditional commodities, goods, and services that create economic interdependence. However, digital interdependence is directly weaponized during conflict, creating cybersecurity risks for the networks negotiating data routes. States do not need to directly prohibit firms from interacting with counterparts across borders – or even possess the capacity to do so – for international security to shape digital interdependence.

To test my theory, I draw on computer network engineering and leverage Internet routing data. The analysis provides robust evidence for the interactions between digital interdependence and power politics. Lowered conflict expectations significantly increase states' digital interdependence through network operators. This effect survives several sensitivity analyses, including dropping treated dyads and controlling for states' economic relationships. I carry out two analyses to show that conflict externalities, rather than state preferences, align digital interdependence and power politics. States can influence digital interdependence through infrastructure investments – I limit the analysis to dyads with existing infrastructure links. States also politicize trade through state-owned enterprises – I limit the analysis to only state-owned networks. The effects of conflict expectations on digital interdependence are not significantly different from the overall effect in either case.

This paper does not address several lines of research. If treaties and alliances increase interdependence, and dense data exchanges benefit the digital economy, Internet-dependent firms may lobby for cooperation consistent with the commercial peace. Hurel and Lobato (2018) discuss technology firms as norm entrepreneurs, focusing on efforts to influence cybersecurity policies and international cybercrime cooperation. The Cybersecurity Tech Accord, which includes some of the largest Internet service providers (BT, Orange, NTT, Telefonica), publishes international guidance on peacemaking in cyberspace and invests in multilateral efforts to ensure cyber stability.

Why test the connection between international security and digital interdependence via potential externalities, rather than actual externalities? Future work should address the effects of cyber externalities (cyberattacks) on digital interdependence. One current challenge is bias in existing cybersecurity incident data (Oppenheimer 2024). A study testing the effects of cyberattacks on digital interdependence would have to assume a high level of reporting by private actors. In the absence of reliable cyberattack data, this paper tests whether conflict expectations influence data routing. Experts clearly believe that worsening relations between states create cyber risks, and security and diplomatic disputes often provoke cyberattacks. However, we currently lack the data to connect cyberattacks and digital interdependence.

The Internet is a vast and complex network. This paper addresses one form of digital interdependence – networks exchanging data traffic – but there are other forms of digital interdependence in different layers of the Internet. For example, companies and users in one country use digital services and platforms from other countries. International security may influence whether platforms allow users to access their services. There is evidence that this occurs through geo-blocking, where websites block all user requests originating from a country's Internet space. For instance, many US-based companies block Cuban users from their platforms (Ablove et al. 2024; Oppenheimer et al. 2024). Alternatively, in line with economic nationalism, users may boycott or avoid top-level domains associated with countries at war. For instance, Georgian Internet users may have avoided '.ru' domains after Russia's invasion in 2008. Future research can

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

theorize and evaluate whether digital interdependence in the Internet's other layers responds to international security.

Power politics shape digital interdependence. Digital interdependence has several distinct features, and states have fewer ways to align firms negotiating data routing with national security policy. However, cybersecurity risks spread through digital interdependence and common attacks are facilitated by data routing. Firms shaping the Internet's structure sit along the front lines of conflict as actors exploit data routes for coercive ends.

Supplementary material. To view supplementary material for this article, please visit https://doi.org/10.1017/S0007123425000328

Data Availability Statement. Replication data and code can be found in Harvard Dataverse: https://doi.org/10.7910/DVN/3NDSF4.

Acknowledgments. I am grateful to Avishay Ben Sasson-Gordis, Adam Breuer, Christina Davis, Rachel Hulvey, Iain Johnston, Joshua Kertzer, Gary King, Abraham Newman, Bruce Schneier, Beth Simmons, Dustin Tingley, and Kevin Troy for their feedback. I also thank the anonymous reviewers and editors for their suggestions. Earlier versions of this paper benefited from the Harvard Government Department International Relations Workshop, the Graduate Students in International Political Economy (GSIPE) series, and the 2022 International Political Economy Society Conference. I would also like to thank the Center for Applied Internet Data Analysis (CAIDA) and KC Claffy for making Internet measurements accessible to researchers.

Financial Support. This research was supported by grants from the Harvard Weatherhead Center for International Affairs.

Competing Interests. None.

References

Ablove A, Chandrashekaran S, Le H, Raman RS, Ramesh R, Oppenheimer H and Ensafi R (2024) Digital Discrimination of Users in Sanctioned States: The Case of the Cuba Embargo. In *33rd USENIX Security Symposium (USENIX Security 24)*, 3909–3926.

Anderson JE (2011) The Gravity Model. *Annual Review of Economics* **3**(1), 133–160.

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

Aronow PM, Samii C and Assenova VA (2015) Cluster-Robust Variance Estimation for Dyadic Data. *Political Analysis* **23**(4), 564–577.

Askari H, Forrer J, Teegen HJ and Yang J (eds) (2003) *Economic Sanctions: Examining Their Philosophy and Efficacy*. Westport, Conn: Praeger.

Baake P and Wichmann T (1999) On the Economics of Internet Peering. *NETNOMICS* **1**(1), 89–105.

Baezner M (2018). Hotspot Analysis: Regional Rivalry between India-Pakistan: Tit-for-Tat in Cyberspace. Center for Security Studies (CSS). ETH: Zurich.

Baldwin DA (1985) *Economic Statecraft*. Princeton, NJ: Princeton University Press.

Baldwin R and Taglioni D (2006). Gravity for Dummies and Dummies for Gravity Equations. NBER Working Paper No. 12516. Cambridge, MA: National Bureau of Economic Research. Doi: 10.3386/w12516.

Baltagi BH, Egger P and Pfaffermayr M (2003) A Generalized Design for Bilateral Trade Flow Models. *Economics Letters* **80**(3), 391–397.

Baltagi BH, Egger P and Pfaffermayr M (2015) Panel Data Gravity Models of International Trade. In Baltagi BH (ed.), *The Oxford Handbook of Panel Data*. Oxford: Oxford University Press, 608–642.

Bearce DH, Flanagan KM and Floros KM (2006) Alliances, Internal Information, and Military Conflict Among Member-States. *International Organization* **60**(3), 595–625.

Besen SM and Israel MA (2013) The Evolution of Internet Interconnection from Hierarchy to 'Mesh': Implications for Government Regulation. *Information Economics and Policy* **25**(4), 235–245.

Blum BS and Goldfarb A (2006) Does the Internet Defy the Law of Gravity? *Journal of International Economics* **70**(2), 384–405.

Box S and West J (2016) Economic and Social Benefits of Internet Openness. OECD Digital Economy Papers, No. 257. Paris: OECD Publishing.

Burri M (2017) The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation. *UC Davis Law Review* 51.

Carisimo E, Gamero-Garrido A, Snoeren AC and Dainotti A (2021) Identifying ASes of State-Owned Internet Operators. In *Proceedings of the 21st ACM Internet Measurement Conference*. IMC '21: ACM Internet Measurement Conference. Virtual Event: ACM, 687–702.

Carlson J, Incerti T and Aronow PM (2024) Dyadic Clustering in International Relations. *Political Analysis* **32**, 186–198.

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

Chavula J, Phokeer A, Formoso A and Feamster N (2017) Insight into Africa's country-level latencies. In *2017 IEEE AFRICON: Science, Technology and Innovation for Africa*. IEEE AFRICON 2017. IEEE, 938–944.

Christin N (2011). *On Critical Infrastructure Protection and International Agreements*. University of Maryland. Working Paper. https://cissm.umd.edu/sites/default/files/2019-07/on_critical_infrastructure_protection_and_international_agreements__033111__final.pdf

Clark DD, Lehr W and Bauer S (2011) Interconnection in the Internet: The Policy Challenge. Available at https://papers.ssrn.com/abstract=1992641 (accessed 23 June 2025). Pre-published.

Clark DH and Reed W (2005) The Strategic Sources of Foreign Policy Substitution. *American Journal of Political Science* **49**(3), 609–624.

Clement A and Obar JA (2015) Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges. In Geist M (ed), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. University of Ottawa Press, 13–44.

Cohen J, Cohen P, West SG and Aiken LS (2003) *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*, 3rd ed. Mahwah, NJ: L. Erlbaum Associates.

Cooper RN (1986) *Economic Policy in an Interdependent World: Essays in World Economics*. Cambridge, Mass: MIT Press.

Cowgill B and Dorobantu C (2014) Worldwide Gravity in Online Commerce.Working Paper.

Czernich N, Falck O, Kretschmer T and Woessmann L (2011) Broadband Infrastructure and Economic Growth*. *The Economic Journal* **121**(552), 505–532.

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

Davis CL, Fuchs A and Johnson K (2019) State Control and the Effects of Foreign Relations on Bilateral Trade. *Journal of Conflict Resolution* **63**(2), 405–438.

De Jonge Oudraat C (2000) Making Economic SanctionsWork. *Survival* **42**(3), 105–128.

Denning DE (2001) Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy. In Arquilla J and Ronfeldt D (eds), *Networks and Netwars. The Future of Terror, Crime and Militancy*. Santa Monica: RAND Corporation.

Deutsch KW (1954) *Political Community at the International Level: Problems of Definition and Measurement*. New York: Doubleday.

DiGiuseppe M and Kleinberg KB (2019) Economics, Security, and Individual-Level Preferences for Trade Agreements. *International Interactions* **45**(2), 289–315.

Dimitropoulos X, Krioukov D, Fomenkov M, Huffaker B, Hyun Y, Claffy K and Riley G (2007) AS Relationships: Inference and Validation. *ACM SIGCOMM Computer Communication Review* **37**(1), 29–40.

Dimitropoulos X, Krioukov D, Huffaker B, Claffy K and Riley G (2005) Inferring AS Relationships: Dead End or Lively Beginning? In Nikoletseas NE (eds) *Experimental and Efficient Algorithms. WEA 2005. Lecture Notes in Computer Science, Workshop on Experimental and Efficient Algorithms* **3503**, 113–125.

Dixit A (2003) Trade Expansion and Contract Enforcement. *Journal of Political Economy* **111**(6), 1293–1317.

Dourado E (2012) Working Paper. Internet Security Without Law: How Service Providers Create Order Online. Mercatus Center.

Dür A, Baccini L and Elsig M (2014) The Design of International Trade Agreements: Introducing a New Dataset. *The Review of International Organizations* **9**(3), 353–375.

Economides N, Majumdar SK, Vogelsang I and Cave ME (2005) The Economics of the Internet Backbone. In *Handbook of Telecommunications Economics*, Vol. **2**. Amsterdam: Elsevier, 373–412.

Edmundson A, Ensafi R, Feamster N and Rexford J (2018) Nation-State Hegemony in Internet Routing. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. COMPASS '18. New York, NY, USA, 1–11.

Fanou R, Francois P and Aben E (2015) On the Diversity of Interdomain Routing in Africa. In Mirkovic J and Liu Y (eds), *Passive and Active Measurement*. Cham: Springer International Publishing, 41–54.

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

Feamster N, Winick J and Rexford J (2004) A Model of BGP Routing for Network Engineering. In *SIGMETRICS '04/ Performance '04*, 12.

Fordham BO (2010) Trade and Asymmetric Alliances. *Journal of Peace Research* **47**(6), 685–696.

Freund C and Weinhold D (2002) The Internet and International Trade in Services. *American Economic Review* **92**(2), 236–240.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Gartzke E (2013) The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security* **38**(2), 41–73.

Gartzke E, Li Q and Boehmer C (2001) Investing in the Peace: Economic Interdependence and International Conflict. *International Organization* **55**(2), 391–438.

Gohdes A (2015) Pulling the Plug: Network Disruptions and Violence in Civil Conflict. *Journal of Peace Research* **52**(3), 352–367.

Gohdes A (2024) *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*. *Disruptive Technology and International Security*. New York: Oxford University Press.

Goldsmith JL and Wu T (2006) *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.

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

Gowa J (1994) *Allies, Adversaries, and International Trade*. Princeton, NJ: Princeton University Press.

Gowa J and Hicks R (2013) Politics, Institutions, and Trade: Lessons of the Interwar Era. *International Organization* **67**(3), 439–467.

Gowa J and Mansfield ED (1993) Power Politics and International Trade. *American Political Science Review* **87**(2), 408–420.

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

Gupta A, Calder M, Feamster N, Chetty M, Calandro E and Katz-Bassett E (2014) Peering at the Internet's Frontier: A First Look at ISP Interconnectivity in Africa. In Faloutsos M and Kuzmanovic A (eds) *Passive and Active Measurement*. Lecture Notes in Computer Science. Cham: Springer International Publishing, 204–213.

Haim DA (2016) Alliance Networks and Trade: The Effect of Indirect Political Alliances on Bilateral Trade Flows. *Journal of Peace Research* **53**(3), 472–490.

Hall C, Anderson R, Clayton R, Ouzounis E and Trimintzios P (2011). Resilience of the Internet Interconnection Ecosystem. ENISA. Available at https://www.cl.cam.ac.uk/~rnc1/weisresilience.pdf (accessed 23 June 2025).

Hall JM (1918) The Effect of War on Contracts. *Columbia Law Review* **18**(4), 325–345.

Harris CW (1961) International Relations and the Disposition of Alien Enemy Property Seized by the United States During World War II: A Case Study on German Properties. *The Journal of Politics* **23**(4), 641–666.

Heilmann K (2016) Does Political Conflict Hurt Trade? Evidence from Consumer Boycotts. *Journal of International Economics* **99**, 179–191.

High-level Panel on Digital Cooperation (2019). The Age of Digital Interdependence. United Nations. Available at https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf (accessed 23 June 2025).

Holme P, Karlin J and Forrest S (2008) An Integrated Model of Traffic, Geography and Economy in the Internet. *ACM SIGCOMM Computer Communication Review* **38**(3), 5–16.

Hui KL, Kim SH and Wang QH (2017) Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly* **41**(2), 497–524.

Hurel LM and Lobato LC (2018) Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs. *Journal of Cyber Policy* **3**(1), 61–76.

Huston G (1998) *ISP Survival Guide*. New York: John Wiley & Sons.

Huston G (2016) The Death of Transit? APNIC Blog, 28 October. Available at https://blog.apnic.net/2016/10/28/the-death-of-transit/ (accessed 23 June 2025).

Jentleson BW (2022) *Sanctions: What Everyone Needs to Know*. *What Everyone Needs To Know*. Oxford: Oxford University Press.

Karlin J, Forrest S and Rexford J (2009) Nation-State Routing: Censorship, Wiretapping, and BGP. doi: 10.48550/arXiv.0903.3218. arXiv: 0903.3218 [cs]. Available at http://arxiv.org/abs/0903.3218 (accessed 23 June 2025). Pre-published.

Keohane RO and Nye JS (1977) *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown and Company.

Keshk OMG, Pollins BM and Reuveny R (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.

Kolkman O, Robachevsky A, Gahnberg C and Badran H (2022) Evolution of the Edge, What about the Internet? In *Proceedings of the ACM SIGCOMM Workshop on Future of Internet Routing & Addressing*. SIGCOMM'22: ACM SIGCOMM 2022 Conference. Amsterdam: ACM, 1–5.

Konte M, Perdisci R and Feamster N (2015) ASwatch: An AS Reputation System to Expose Bulletproof Hosting ASes. *ACM SIGCOMM Computer Communication Review* **45**(4), 625–638.

Kostyuk N and Zhukov YM (2019) Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution* **63**(2), 317–347.

Leeds BA (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 BA, Ritter JM, Mitchell SM and Long AG (2002) Alliance Treaty Obligations and Provisions, 1815-1944. *International Interactions* **28**, 237–260.

Lin H (2012) Escalation Dynamics and Conflict Termination in Cyberspace. *Strategic Studies Quarterly* **6**(3), 46–70.

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Linnemann H (1966) *An Econometric Study of International Trade Flows*. Amsterdam: North-Holland Pub. Co.

Lodhi A and Dovrolis C (2010) A Network Formation Model for Internet Transit Relations. In *Proceedings of the 2010 Workshop on Economics of Networks, Systems, and Computation - NetEcon '10*. The 2010 Workshop. Vancouver, British Columbia, Canada: ACM Press.

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

Long AG, Nordstrom T and Baek K (2007) Allying for Peace: Treaty Obligations and Conflict between Allies. *The Journal of Politics* **69**(4), 1103–1117.

Lopez Gonzalez J and Ferencz J (2018) Digital Trade and Market Openness. *OECD Trade Policy Papers* No. 217. Paris: OECD Publishing. doi:10.1787/1bd89c9a-en. Available at https://www.oecd.org/en/publications/digital-trade-and-market-openness_1bd89c9a-en.html (accessed 23 June 2025).

Luckie M, Huffaker B, Dhamdhere A, Giotsas V and Claffy KC (2013) AS Relationships, Customer Cones, and Validation. In *Proceedings of the 2013 Conference on Internet Measurement Conference*. IMC'13: Internet Measurement Conference. Barcelona Spain: ACM, 243–256.

Lupu Y and Poast P (2016) Team of Former Rivals: A Multilateral Theory of Non-Aggression Pacts. *Journal of Peace Research* **53**(3), 344–358.

Maida EM (2013) *The Regulation of Internet Interconnection: Assessing Network Market Power*. Masters' thesis, Massachusetts Institute of Technology.

Mansfield ED and Bronson R (1997) Alliances, Preferential Trading Arrangements, and International Trade. *American Political Science Review* **91**(1), 94–107.

Marcos P, Chiesa M, Dietzel C, Canini M and Barcellos M (2020) A Survey on the Current Internet Interconnection Practices. *ACM SIGCOMM Computer Communication Review* **50**(1), 10–17.

Mattes M and Vonnahme G (2010) Contracting for Peace: Do Nonaggression Pacts Reduce Conflict? *The Journal of Politics* **72**(4), 925–938.

Meier-Hahn U (2016) Exploring the Regulatory Conditions of Internet Interconnection – A Survey Among Internet Interconnection Professionals. Available at https://papers.ssrn.com/abstract = 2740312 (accessed 23 June 2025). Pre-published.

Meier-Hahn U (2017) The Secrets of De-Peering. RIPE Labs, 6 August. Available at https://labs.ripe.net/author/uta_meier_hahn/the-secrets-of-de-peering/ (accessed 23 June 2025).

Michaels G and Zhi X (2010) Freedom Fries. *American Economic Journal: Applied Economics* **2**(3), 256–281.

Moore D, Paxson V, Savage S, Shannon C, Staniford S and Weaver N (2003) Inside the Slammer Worm. *IEEE Security & Privacy* **1**(4), 33–39.

Morgan TC and Bapat NA (2003) Imposing Sanctions: States, Firms, and Economic Coercion. *International Studies Review* **5**(4), 65–79.

Morrow JD (1994) Alliances, Credibility, and Peacetime Costs. *Journal of Conflict Resolution* **38**(2), 270–297.

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

Mueller JE (1970) Presidential Popularity from Truman to Johnson. *American Political Science Review* **64**(1), 18–34.

Mulder N (2022) *The Economic Weapon: The Rise of Sanctions as a Tool of Modern War*. New Haven: Yale University Press.

Mustafa S, Dey PK and Yuksel M (2022) Peer Me Maybe?: A Data-Centric Approach to ISP Peer Selection. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. Budapest, Hungary: IEEE, 1–9.

Nazario J (2009) Politically Motivated Denial of Service Attacks. In Czosseck C and Geers K (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press, 163–181.

Nguyen D and Paczos M (2020) OECD Digital Economy Papers. Measuring the Economic Value of Data and Cross-Border Data Flows. 297. OECD. Available at https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/08/measuring-the-economic-value-of-data-and-cross-border-data-flows_219e1b8b/6345995e-en.pdf (accessed 23 June 2025).

Nicholson J and McHenry G (2016). *Measuring the Value of Cross-Border Data Flows*. U.S. Department of Commerce.

Norton WB (2014) *The 2014 Internet Peering Playbook: Connecting to the Core of the Internet*. Palo Alto, CA: DrPeering Press.

O'Hara K and Hall W(2021) *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. New York: Oxford University Press.

Office of Public Affairs (2020) *Team Telecom Recommends That the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States*. Department of Justice. Available at https://www.justice.gov/archives/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea (accessed 23 June 2025).

Oppenheimer H (2025) Replication Data for: Digital Interdependence and Power Politics. https://doi.org/10.7910/DVN/3NDSF4, Harvard Dataverse, V1.

Oppenheimer H (2024) How the Process of Discovering Cyberattacks Biases Our Understanding of Cybersecurity. *Journal of Peace Research* **61**(1), 28–43.

Oppenheimer H, Ablove A and Ensafi R (2024) How Geoblocking Limits Digital Access in Sanctioned States. *Lawfare*, 18 November. Available at https://www.lawfaremedia.org/article/how-geoblocking-limits-digital-access-in-sanctioned-states (accessed 23 June 2025).

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press

Ortwein A, Bock K and Levin D (2023) Towards a Comprehensive Understanding of Russian Transit Censorship. In *Free and Open Communications on the Internet 2023.* vol **2**.

Owsiak AP and Frazier DV (2014) The Conflict Management Efforts of Allies in Interstate Disputes. *Foreign Policy Analysis* **10**(3), 243–264.

Parker SL (1995) Towards an Understanding of 'Rally' Effects: Public Opinion in the Persian Gulf War. *Public Opinion Quarterly* **59**(4), 526–546.

Polachek SW(1980) Conflict and Trade. *Journal of Conflict Resolution* **24**(1), 55–78.

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

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

Pressman J (2012) *Warring Friends: Alliance Restraint in International Politics*. Cornell Studies in Security Affairs. Ithaca, NY: Cornell University Press.

Rid T (2013) *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Roberts ME (2018) *Censored: Distraction and Diversion inside China's Great Firewall.* Princeton, NJ: Princeton University Press.

Rosa FR (2021) Internet Interconnection Infrastructure: Lessons from the Global South. *Internet Policy Review* **10**(4), 2–22.

Rosecrance R and Stein A (1973) Interdependence: Myth or Reality. *World Politics* **26**(1), 1–27.

Santos Silva JMC and Tenreyro S (2006) The Log of Gravity. *The Review of Economics and Statistics* **88**(4), 641–658.

Savage IR and Deutsch KW (1960) A Statistical Model of the Gross Analysis of Transaction Flows. *Econometrica* **28**(3), 551–572.

Schumann R and Kende M (2013) *Lifting Barriers to Internet Development in Africa: Suggestions for Improving Connectivity*. Report for the Internet Society. Available at https://www.internetsociety.org/wp-content/uploads/2017/08/Barriers20to20Internet20in20Africa20Internet20Society_0.pdf (accessed 23 June 2025).

Sermpezis P (2022) Bias in Internet Measurement Infrastructure. RIPE Labs. Available at https://labs.ripe.net/author/pavlos_sermpezis/bias-in-internet-measurement-infrastructure/ (accessed 23 June 2025).

Singer HJ (2014) *Mandatory Interconnection: Should the FCC Serve as Internet Traffic Cop?* Policy Brief, *Progressive Policy Institute*. Available at https://www.progressivepolicy.org/wp-content/uploads/2014/05/2014.05-Singer_Mandatory-Interconnection_Should-the-FCC-Serve-as-Internet-Traffic-Cop.pdf (accesses 23 June 2025).

Smith A (1995) Alliance Formation and War. *International Studies Quarterly* **39**(4), 405–425.

Smith A (1998) Extended Deterrence and Alliance Formation. *International Interactions* **24**(4), 315–343.

Starosielski N (2015) *The Undersea Network*. Durham: Duke University Press.

The CAIDA UCSD AS Relationships Dataset, 2010-2018 (2013). CAIDA. Available at https://www.caida.org/catalog/datasets/as-relationships/ (accessed 23 June 2025).

The CAIDA UCSD Inferred AS to Organization Mapping Dataset, 2010-2018 (2014). CAIDA. Available at https://www.caida.org/catalog/datasets/as-organizations/ (accessed 23 June 2025).

Tinbergen J (1962) *Shaping the World Economy: Suggestions for an International Economic Policy*. New York: Twentieth Century Fund.

Trentmann F (2019) Consumer Boycotts in Modern History: States, Moral Boundaries, and Political Action. In Feldman D (ed.), *Boycotts Past and Present*. Cham: Springer International Publishing, 21–39.

Valeriano B and Maness RC (2015) *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.

Warren TC (2016) Modeling the Coevolution of International and Domestic Institutions: Alliances, Democracy, and the Complex Path to Peace. *Journal of Peace Research* **53**(3), 424–441.

Weidner M and Zylkin T (2021) Bias and Consistency in Three-Way Gravity Models. *Journal of International Economics* **132**, 103513.

Weitsman PA (2004) *Dangerous Alliances: Proponents of Peace, Weapons of War*. Stanford, CA: Stanford University Press.

Weller and Woodcock B (2013) Internet Traffic Exchange: Market Developments and Policy Challenges. *OECD Digital Economy Papers*, No. 207. Paris: OECD Publishing.

Weymouth S (2023) *Digital Globalization: Politics, Policy, and a Governance Paradox. Cambridge Elements in International Relations*. Cambridge: Cambridge University Press.

Woodcock B and Frigino M (2021) Survey of Internet Carrier Interconnection Agreements. Packet Clearing House.

Yang Y and Zhang H (2023) Three-Way Gravity Models with Multiplicative Unobserved Effects. *The Econometrics Journal* **26**(3), 422–443.

Zhuo R, Huffaker B, Claffy KC and Greenstein S (2021) The Impact of the General Data Protection Regulation on Internet Interconnection. *Telecommunications Policy* **45**(2).

Cite this article: Oppenheimer H (2025) Digital Interdependence and Power Politics. *British Journal of Political Science* 1–23. https://doi.org/10.1017/S0007123425000328

https://doi.org/10.1017/S0007123425000328 Published online by Cambridge University Press