Weaponized Interdependence: How Global Economic Networks Shape Coercion and Surveillance

Henry Farrell and Abraham Newman

Forthcoming, *International Security* (Summer 2019)

Henry Farrell is a Professor of Political Science and International Affairs at George Washington University. Abraham Newman is a Professor at the Edmund A. Walsh School of Foreign Service at Georgetown University. The authors are grateful to Miles Evers, Llewellyn Hughes, Erik Jones, Miles Kahler, Matthias Matthijs, Kathleen McNamara, Gideon Rose, Mark Schwartz, William Winecoff, as well as the reviewers for comments and criticism. Charles Glaser provided especially detailed and helpful comments on an early draft. Previous versions of this article were presented at the International Studies Association annual meeting in 2018, and at the Johns Hopkins University School of Advanced International Studies Research Seminar in Politics and Political Economy on April 17, 2018. They are also grateful to the participants and audience at both events for feedback.

Abstract: Liberals claim that globalization has led to fragmentation and decentralized networks of power relations. This does not explain how states increasingly 'weaponize interdependence' by leveraging global networks of informational and financial exchange for strategic advantage. We explain how weaponized interdependence works. We begin from the theoretical literature on network topography, showing how standard models predict that many networks grow asymmetrically so that some nodes are far more connected than others. This nicely describes several key global economic networks, centering on the US and a few other states. Highly asymmetric networks allow states with (1) effective jurisdiction over the key nodes, and (2) appropriate domestic institutions, to weaponize their structural advantages through two mechanisms. First, they can employ the 'panopticon effect' to gather strategically valuable information. Second, they can employ the 'chokepoint effect' to deny network access to adversaries. We test these arguments' plausibility across two extended case studies that provide variation both in the extent of US jurisdiction and in domestic institutions – the SWIFT financial messaging system, and the Internet, finding that the outcomes match the framework's predictions well. We conclude by discussing the policy implications, and the strategies targeted states may use to insulate themselves.

In May 2018, Donald Trump announced that the United States was pulling out of the Joint Comprehensive Plan of Action agreement on Iran's nuclear program and reimposing sanctions. Most notably, many of these penalties apply not to U.S. firms, but to foreign firms that may have no presence in the U.S. The sanctions are consequential in large part because of U.S. importance to the global financial network.[1] This unilateral action led to protest among the United States' European allies: France's finance minister, Bruno Le Maire, for example, tartly noted that the United States was not the "economic policeman of the planet."[2] In particular, the U.S. and Europe disagreed over whether Iran should be cut out of the SWIFT messaging network, which allows banks to communicate with each other about financial transfers, and is a core component of the global financial system.

The reimposition of sanctions on Iran is just one recent example of how the US is using global economic networks to achieve its strategic aims.[3] While security scholars have long recognized the crucial importance of energy markets in shaping geostrategic outcomes,[4] financial and information markets are rapidly coming to play similarly important roles. In Rosa Brooks's

---

[1] The legal principles through which exposure is determined are complex. For a useful brief introduction, see Serena B. Wille, "Anti-Money-Laundering and OFAC Sanctions Issues," *CFA Institute Conference Proceedings Quarterly* Vol. 29, No. 3 (2011), pp. 59-64.

[2] Anne-Sylvaine Chassany, Michael Peel and Tobias Buck, "EU to Seek Exemptions from New US Sanctions on Iran," *Financial Times* (London: Financial Times May 9 2018), https://www.ft.com/content/d26ddea6-5375-11e8-b24e-cad6aa67e23e.

[3] Henry Foy, "EN+ President Steps Down in Move to Win US Sanctions Waiver," *Financial Times* (London: Financial Times, June 4, 2018), https://www.ft.com/content/8c1ac0a6-67be-11e8-8cf3-0c230fa67aec.rusal

[4] Llewelyn Hughes and Austin Long, "Is There an Oil Weapon? Security Implications of Changes in the Structure of the International Oil Market," *International Security* Vol. 39, No. 3 (Winter 2014/2015), pp. 152-189; Jeff D. Colgan, "Fueling the Fire: Pathways from Oil to War," *International Security*, Vol. 38, No. 2 (Fall 2013), pp.147-180, Charles L. Glaser, "How Oil Influences U.S. National Security: Reframing Energy Security," *International* Security, Vol. 38, No.2 (Fall 2013), pp. 112-146; Llewelyn Hughes and Phillip Y. Lipscy, "The Politics of Energy," *Annual Review of Political Science* Vol. 16, No. 1 (2013), pp. 449-469.

evocative description, globalization has created a world in which everything became war.[5] Flows of finance, information, and physical goods across borders create both new risks for states and new tools to alternatively exploit or mitigate those risks. The result, as Thomas Wright, describes it, is a world where unprecedented levels of interdependence are combined with continued jockeying for power, so that states that are unwilling to engage in direct conflict may still employ all measures short of war.[6]

Global economic networks have security consequences because they increase interdependence between states that were previously relatively autonomous. Yet, existing theory provides few guideposts as to how states may leverage network structures as a coercive tool and under what circumstances. It has focused instead on trade relations between dyadic pairs and the vulnerabilities generated by those interactions.[7] Similarly, work on economic sanctions has yet to fully grasp the consequences of economic networks and how they are being weaponized. Rather, that literature primarily looks to explain the success or failure of direct sanctions (i.e. sanctions which involve states denying outside access to their own markets individually or as an alliance).[8]

---

[5] Rosa Brooks, *How Everything Became War and the Military Became Everything* (New York, NY.: Simon and Schuster 2017).

[6] Thomas J. Wright, *All Measures Short of War: The Contest for the Twenty-First Century and the Future of American Power* (New Haven, CT.: Yale University Press 2017).

[7] Joanne Gowa, "Bipolarity, Multipolarity, and Free Trade," *American Political Science Review*, Vol. 83, No.4 (1989), pp 1245-1256; Brian M. Pollins, "Does Trade Still Follow the Flag?," *American Political Science Review* Vol. 83, No. 2 (1989), pp. 465-480; John R. Oneal, Frances H. Oneal, Zeev Maoz, and Bruce Russett. "The Liberal Peace: Interdependence, Democracy, and International Conflict, 1950-85," *Journal of Peace Research*, Vol. 33, No. 1 (1996), pp. 11-28; Copeland, Dale C. *Economic Interdependence and War*. Princeton: Princeton University Press, 2014.

[8] Robert A. Pape, "Why Economic Sanctions Do Not Work," *International Security* Vol. 22, No. 2 (1997), pp. 90-136; Kimberly Ann Elliott, "The Sanctions Glass: Half Full or Completely Empty?," *International Security,* Vol. 23, No. 1 (1998), pp. 50-65; Daniel W. Drezner. *The Sanctions Paradox: Economic Statecraft and International Relations* (New York: Cambridge University Press, 1999); David A. Baldwin, "The Sanctions Debate and the Logic of Choice," *International Security*, Vol. 24, No. 3 (2000), pp. 80-107; Jonathan Kirshner, "Review Essay:

Power and vulnerability are characterized as the consequences of aggregate market size or bilateral interdependencies. In addition, accounts that examine more diffuse or secondary sanctions have focused more on comparative effectiveness than on theory building.[9]

In this article, we develop a different understanding of state power, which highlights the structural aspects of interdependence. Specifically, we show how the topography of the economic networks of interdependence intersect with domestic institutions and norms to shape coercive authority. Our account places networks such as financial communications, supply chains, and the Internet, which have gone largely neglected by international relations scholars, at the heart of a compelling new understanding of globalization and power.[10] Globalization has

---

Economic Sanctions: The State of the Art," *Security Studies* Vol. 11, No. 4 (2002), pp. 160-179; Fiona McGillivray, and Allan C. Stam. "Political Institutions, Coercive Diplomacy, and the Duration of Economic Sanctions," *Journal of Conflict Resolution* Vol. 48, No. 2 (2004), pp. 154-172. Daniel Drezner, "Outside the Box: Explaining Sanctions in Pursuit of Foreign Economic Goals," *International Interactions*, Vol.26, No.4 (2001), pp. 379-410 does consider secondary sanctions, as does the policy literature we discuss below.

[9] See Peter D. Feaver and Eric B. Lorber, *Coercive Diplomacy and the New Financial Levers: Evaluating the Intended and Unintended Consequences of Financial Sanctions* (London: Legatum Institute 2010); Orde F. Kittrie, "New Sanctions for a New Century: Treasury's Innovative Use of Financial Sanctions," *University of Pennsylvania Journal of International Law*, Vol. 30, No. 1 (2008), pp.789-822; Daniel Drezner, "Targeted Sanctions in a World of Global Finance," *International Interactions*, Vol. 41 (2015), pp. 755-64. Secondary sanctions co-exist with other tools to control international financial flows. For a useful recent overview, see Miles Kahler, Maya Forstater, Michael G. Findley, Jodi Vittori, Erica Westenberg, and Yaya J. Fanusie, *Global Governance to Combat Illicit Financial Flows: Measurement, Evaluation, Innovation* (Washington DC: Council on Foreign Relations 2018).

[10] Of course, there is a burgeoning scholarship on cybersecurity, which is relevant to the Internet. See, for a few recent examples, Sarah Kreps and Jacquelyn Schneider, *Escalation Firebreaks in the Cyber, Conventional and Nuclear Domains: Moving Beyond Effects-Based Logics* (unpublished paper); Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* (2017) Vol. 41, No.3, pp.44-71; Rebecca Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes and Assessment," *International Security* (2017), Vol. 41, No. 3, pp. 72-109; Henry Farrell and Charles Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* (2017) Vol.3, No.1, pp.7-17; Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* (2015) Vol. 39, No. 3, pp.7-47. However, this literature largely fails to address the network characteristics of the Internet, instead focusing on variation in traditional metrics such as the offense-defense

transformed the liberal order, by moving the action away from multilateral interstate negotiations, and towards networks of private actors.[11] This has had crucial consequences for where state power is located in international politics, and how it is exercised.

We contrast our argument with standard liberal accounts of complex interdependence. The initial liberal account of interdependence paid some attention to power, but emphasized bilateral relationships. Subsequent liberal accounts have tended either to avoid the question of power, focusing on mutual cooperative gains, to suggest that apparently lopsided global networks obscure more fundamental patterns of mutual dependence, or to posit a networked global order in which liberal states such as the US can exercise "power with" (the power to work together constructively with allies) to achieve liberal objectives.[12]

---

balance, and the ability to deter or compel, tending to treat the network characteristics of the Internet either as a constant, or a straightforward determinant of state-level vulnerability or strength (so that technologically advanced states such as the US will have a different set of strengths and vulnerabilities than states which rely less on technology). An earlier proto-literature on 'netwar' examines how leaderless networks are becoming more important in world politics, but is primarily descriptive in nature. See John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica: Rand Corporation 1996). There is a technical literature that discusses networks, but it tends not to discuss the strategic aspects we focus on below. For an important exception, see Réka Albert, Hawoong Jeong, and Albert-László Barabási, "Error and Attack Tolerance of Complex Networks;" *Nature*, Vol. 406, No. 6794 (2000), pp. 378-382.

[11] Kathryn Judge, "Intermediary Influence," *University of Chicago Law Review*, Vol. 82, No. 2, pp. 573-642.

[12] See Robert O. Keohane and Joseph S. Nye, *Power and Interdependence* (Fourth Edition) (New York, NY: Longman 2012), Kal Raustiala,"The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law," *Virginia Journal of International Law* Vol. 43, No.1 (2002), pp.1-92; Anne-Marie Slaughter, "Global Government Networks, Global Information Agencies, and Disaggregated Democracy," *Michigan Journal of International Law* (2002), Vol. 24, pp.1044-1075; Anne-Marie Slaughter, *A New World Order* (Princeton NJ: Princeton University Press 2004); Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World* (New Haven, CT: Yale University Press 2017). The classic critique of liberalism's emphasis on mutual gains from cooperation is Stephen D. Krasner, "Global Communications and National Power: Life on the Pareto Frontier," *World Politics* Vol. 43, No. 3 (1991), pp.336-366.

Our alternative account makes a starkly different assumption, providing a structural account of interdependence in which network topography generates enduring power imbalances among states. Here we draw on sociological and computational research on large-scale networks, which demonstrate the tendency of complex systems to produce asymmetric network structures, in which some nodes are "hubs," and are far more connected than others.[13]

Asymmetric network structures create the potential for "weaponized interdependence," in which some states are able to leverage interdependent relations to coerce others. Specifically, states with political authority over the central nodes in the international networked structures through which money, goods, and information travel are uniquely positioned to impose costs on others. If they have appropriate domestic institutions, they can weaponize networks to gather information or choke off economic and information flows, discover and exploit vulnerabilities, compel policy change, and deter unwanted actions. We identify and explain variation in two strategies through which states can gain powerful advantages from weaponizing interdependence, which rely on the panopticon and chokepoint effects of networks. In the former, network position is used to extract informational advantages vis-à-vis adversaries, whereas in the latter, advantaged states can cut adversaries off from network flows.

[13]Albert-László Barabási and Réka Albert. "Emergence of Scaling in Random Networks," *Science* Vol. 286, No. 5439 (1999), pp. 509-512; Mark E. J. Newman and Juyong Park, "Why Social Networks are Different from Other Types of Networks," *Physical Review E* Vol. 68, No. 036122 (2003), pp.1-8; Aaron Clauset, Cosma Rohilla Shalizi, and Mark E.J. Newman. "Power-Law Distributions in Empirical Data." *SIAM Review* Vol. 51, No. 4 (2009), pp. 661-703. Emilie Hafner-Burton, Miles Kahler, and Alexander H. Montgomery. "Network Analysis for International Relations," *International Organization* (2009), Vol. 63, No. 3, pp. 559-592; Stacie E. Goddard, "Embedded Revisionism: Networks, Institutions, and Challenges to World Order." *International Organization* (2018): 1-35.

To test the plausibility of our argument, we present detailed analytic narratives of two substantive areas – financial messaging and Internet communications.[14] We selected these areas as they are significant to a range of critical security issues including rogue state non proliferation, counter terrorism, and great power competition. Moreover, global finance and the Internet are often described as highly decentralized in the international political economy literature. As such, they offer an important test of our argument and a contrast to the more common liberal perspective on global market interactions.

At the same time, financial messaging and Internet communication see important variation in the level and kind of control that they offer to influential states. In the former, the US – in combination with its allies – has sufficient jurisdictional grasp and appropriate domestic institutions to oblige hub actors to provide them with information and to cut off other actors and states. In Internet communications, the US solely has appropriate jurisdictional grasp and appropriate institutions to oblige hub actors to provide it with information, but does not have domestic institutions that would allow it to demand that other states be cut out of the network. This would lead us to expect that in the case of financial messaging, the US and its allies will be able to exercise both the panopticon and chokepoint effects – so long as they agree. In contrast, in Internet communications, the US will be able to exercise the panopticon effect even without the consent of its allies, but will not be able to exercise the chokepoint effect. This variation allows us to demonstrate the limits of these network strategies and also show that they are not simply coterminous with US market size or military power. Empirically, the cases draw on

[14] Anecdotal evidence suggests similar processes are at work in a number of other areas including dollar clearing and global supply chains. See, for example, Cheng Ting-Fang and Lauly Li, "'Huawei Freeze' chills global supply chain," *Nikki Asian Review*, December 8 (2018).

extensive readings of the primary and secondary literature as well as interviews with key policy-makers.

Our argument has significant implications for scholars interested in thinking about the future of conflict in a world of global economic and information networks. For those steeped in the liberal tradition, we demonstrate that institutions designed to generate market efficiencies and reduce transaction costs can be deployed for coercive ends. Focal points of cooperation have become sites of control. For those researchers interested in conflict studies and power, we show the critical role that economic relations play in coercion. Rather than rehashing more conventional debates on trade and conflict, we underscore how relatively new forms of economic interaction – financial and information flows – shape strategic opportunities, stressing in particular how the topography of global networks structures coercion. Here, we use basic insights from network theory to rethink structural power, linking the literatures on economic and security relations to show how coercive economic power can stem from structural characteristics of the global economy. Finally, the article begins to map the deep empirical connections between economic networks – for example, financial messaging, dollar clearing, global supply chains, and Internet communication – and a series of pressing real-world issues – counterterrorism, cybersecurity, rogue states, and great power competition.

We begin by explaining how global networks play a structural role in the world economy. Next, we describe how these networks, together with domestic institutions and norms, shape the strategic options available to actors, focusing on what we describe as the panopticon and chokepoint effects. We provide detailed parallel histories of how networks in financial communication and internet communication developed and were weaponized by the US. We

conclude by considering the policy implications of clashes between states such as the U.S. that have weaponized interdependence and other states looking to counter these influences.

Statecraft and Structure: The Role of Global Networks

As globalization has advanced, it has fostered new networks of exchange – whether economic, informational, or physical – that have remade domestic economies, densely and intimately interconnecting them in ways that are nearly impossible to unravel.[15] The financial sector depends on international messaging networks, which have become the key means through which domestic banks and financial institutions arrange transfers and communicate with each other. Informational networks such as the Internet are notoriously internationalized – a single web page can stitch together content and advertisements from myriad independent servers, perhaps located in different countries. Physical manufacture depends on vast tangled supply chains that extend globally, greatly complicating trade wars, since high tariffs on importers are likely to damage the interests of domestic suppliers.

Such networks have typically been depicted by liberals as a form of "complex interdependence," a fragmented polity in which "there were multiple actors (rather than just states), multiple issues that were not necessarily hierarchically ordered, and force and the threat of force were not valuable tools of policy."[16] Such arguments allowed some space for the exercise of bilateral power, showing how states that depended on imports from other states, and

[15] Recent scholarship in international political economy has begun to focus more explicitly on the relationship between structure and statecraft. For a network based critique of state level reductionism similar to ours, see Thomas Oatley, "The Reductionist Gamble: Open Economy Politics in the Global Economy*." International Organization* Vol. 65, No. 2 (2011), pp. 311-341.
[16] Pp. 36-37, Robert O. Keohane, "The Old IPE and the New," *Review of International Political Economy* Vol. 16, No.1 (2009), pp. 34-46.

had no ready substitutes, were vulnerable to outside pressure. However, liberal scholars stressed the power resources of actors rather than structural factors, in particular the dispersion of power across such networks, and often emphasized how interdependence generated reciprocal rather than one-sided vulnerabilities.

As globalization progressed, liberals have continued to argue that global networks result in reciprocal dependence, which tends to make coercive strategies less effective. Thus, for example, Robert Keohane and Joseph Nye describe globalization as involving the development of "networks of interdependence." Although they accept that, as a "first approximation," the US appears to be a hub in these networks, they also argue that it would be a "mistake to envisage contemporary networks of globalism simply in terms of a hub and spokes of an American empire that creates dependency for smaller countries."[17] Instead, Keohane and Nye suggest that vulnerabilities are reciprocal and that there are multitudes of different possible hubs, reducing the dominance of great powers such as the US. Furthermore, they argue that asymmetries are likely to diminish over time as "structural holes" are filled in.[18] More recently, Nye has argued that "entanglement" between states' economic and information systems can have important pacifying benefits for cybersecurity: precisely because states are interdependent, they are less liable to launch attacks that may damage themselves as well as their adversaries.[19]

Other liberal scholars, such as Anne-Marie Slaughter, claim that globalization creates decentralized networks that generate new opportunities for cooperative diplomacy.[20] Slaughter's guiding metaphor for globalization is a network of points that are intimately connected by a

[17] P.253, Keohane and Nye, *Power and Interdependence*.
[18] Ibid.
[19] Nye, "Deterrence and Dissuasion in Cyberspace."
[20] Raustiala, "The Architecture of International Cooperation," Slaughter, *The New World Order* and *The Chessboard and the Web*.

"web" rather than a "chessboard." An arbitrarily large number of paths may connect two or several of these points together, suggesting that globalization is best understood as a nonhierarchical network in which the new arts of diplomacy consist in identifying the right relationships among the multitudes of possibilities to accomplish a given task. In such a network, liberals such as Slaughter argue, power is "power with," rather than "power over."[21]

Like these liberal accounts, our approach takes networks seriously. However, it starts from different premises about their genesis and consequences. First, we argue that networks are structures in the sociological sense of the term, which is to say that they shape what actors can or cannot do. An important body of emerging scholarship in international political economy, which we dub the New Structuralism, looks to understand the consequences of globally emergent phenomena for states and other actors.[22] In the longer term, such networks may change, but in the short to medium term they are self-reinforcing and resistant to efforts to disrupt them.

Second, network structures can have important consequences for the distribution of power. In contradistinction to liberal claims, they do not produce a flat or fragmented world of diffuse power relations and ready cooperation, nor do they tend to become less asymmetric over time. Instead, they result in a specific, tangible, and enduring configuration of power imbalance. Key global economic networks – like many other complex phenomena – tend to generate ever more asymmetric networks in which exchange becomes centralized, flowing through a few

[21] P.163, Slaughter, *The Chessboard and the Web*.
[22] See in particular Stacie E. Goddard, and Daniel H. Nexon, "The dynamics of global power politics: A framework for analysis." *Journal of Global Security Studies* Vol. 1, No. 1 (2015), pp. 4-18, Mark Blyth and Matthias Matthijs, "Black Swans, Lame Ducks and the Mystery of IPE's Missing Macroeconomy," *Review of International Political Economy*, Vol. 24, No. 2 (2017), pp. 203-31, Seva Gunitsky (2013), "Complexity and Theories of Change in World Politics," International Theory Vol.5, No.1, pp. 35-63 and Thomas Oatley, "Towards a Political Economy of Complex Interdependence," *European Journal of International Relations* (forthcoming).

specific intermediaries.[23] Contrary to Keohane and Nye's predictions, key global economic networks have converged towards "hub and spoke" systems with important consequences for power relations.[24]

Networks can be described more formally. Network theory starts from the basis that networks involve two elements – the "nodes," each representing a specific actor or location within the network, and the "ties" (sometimes called edges), or connections between nodes, which channel information, resources, or other forms of influence. In simple representations, these ties are assumed to carry resources or influence in both directions. The "degree" of a node is the number of ties that connect it to other nodes – the higher the degree, the more connections it enjoys. Empirically, these nodes may be specific physical entities such as the computers that run Internet exchanges or institutions such as a particular bank. The pattern of nodes and links between them is the topography (or what international relations scholars might call the "structure") of the network.

In our account, as in other structural accounts such as neorealism, network structures are the consequence of the accumulated actions of myriad different actors, which aggregate to produce structures that influence their behavior. Specifically, the market-focused strategies of

---

[23] John Padgett and Christopher K. Ansell. "Robust Action and the Rise of the Medici, 1400-1434." *American Journal of Sociology* Vol. 98, No. 6 (1993), pp. 1259-1319, Judge, "Intermediary Influence".

[24] Our arguments can be seen as a specific application of Susan Strange's notion of "structural power." See, for example Susan Strange, *The Retreat of the State: The Diffusion of Power in the World Economy* (New York: Cambridge University Press 1996). See also Susan K. Sell, "Ahead of Her Time? Susan Strange and Global Governance," in *Susan Strange and the Future of Global Political Economy,* ed. Randall Germain, London: Routledge 2016. For different accounts, see Philip Cerny, *Rethinking World Politics: A Theory of Transnational Pluralism* (New York: Oxford University Press 2010) and Louis W. Pauly, "The Anarchical Society and a Global Political Economy," in *The Anarchical Society at 40*, ed. Hidemi Suganami, Madeline Carr and Adam Humphreys (New York: Oxford University Press 2017). On network power, political theory and international relations more generally, see David Singh Grewal, *Network Power: The Social Dynamics of Globalization* (New York: Oxford University Press 2009).

business actors lead, inadvertently or otherwise, to highly centralized global networks of communication, exchange, and physical production. Asymmetric growth means that globalization – like other networked forms of human activity[25] – generates networks with stark inequality of influence.[26] The distribution of degree (i.e, of links across nodes) may approximate to a power law, or a log normal distribution, or a stretched exponential depending on particulars.[27] For the purposes of our argument, the exact statistical classification of the distributions is irrelevant – what is important is that social networks tend to be highly unequal.

Such inequalities may arise in a number of plausible ways. Simple models of preferential attachment suggest that as networks grow, new nodes are slightly more likely to attach to nodes that already have many ties than to nodes that have fewer such ties. As a result, sharply unequal

[25] Newman and Park, "Why Social Networks." An important literature in statistical physics and related disciplines studies the topology of large scale networks, and how topology shapes e.g. processes of contagion. See Duncan Watts, "The 'New' Science of Networks," *Annual Review of Sociology* (2004), Vol. 30, pp.243-270 for a useful overview, and Mark Newman, Albert-László Barabási, and Duncan J. Watts (eds.), *The Structure and Dynamics of Networks*, (Princeton, NJ: Princeton University Press, 2011) for an excellent selection of important work. This literature has been underused by political scientists. For recent exceptions, see Emilie Hafner-Burton, Miles Kahler, and Alexander H. Montgomery. "Network Analysis for International Relations,"; Stacie Goddard, "Embedded Revisionism"; Miles Kahler, Network Politics: Agency, Power, and Governance (Ithaca: Cornell University Press 2009); Oatley, Thomas, *A Political Economy of American Hegemony* (New York: Cambridge University Press 2015); Kinne, Brandon J. "Defense Cooperation Agreements and the Emergence of a Global Security Network." *International Organization* 72, no. 4 (2018): 799-837.

[26] Of course, some forms of international exchange are not networks in this sense – market transfers of commodities with a significant number of suppliers, and with no need for network infrastructure are not likely to be subject to the dynamics we discuss here. We return to this point in the conclusion.

[27] See Clauset, Shalizi, and Newman. "Power-Law Distributions in Empirical Data." For applications to security, see Aaron Clauset, Maxwell Young and Kristian Skrede Gleditsch, "On the Frequency of Severe Terrorist Events," *Journal of Conflict Resolution* Vol. 51, No.1 (2007), pp. 58-88, and Aaron Clauset, "Trends and Fluctuations in the Severity of Interstate Wars,'' *Science Advances* Vol. 4, No. 2 (2018), pp.1-9.

distributions are likely to emerge over time.[28] Network effects, in which the value of a service to its users increases as a function of the number of users already using it, may lead actors to converge on networks that already have many participants, while efficiency concerns lead the network providers to create hub-and-spoke systems of communication. Finally, innovation research suggests that there are important learning-by-doing effects, in which central nodes in networks have access to more information and relationships than other members of the network, causing others to link to them preferentially to maintain access to learning processes.[29]

These mechanisms and others may generate strong rich-get-richer effects over the short to medium term, in which certain nodes in the network become more central in the network than others. The networks they generate are structural in the precise yet limited sense that after they have emerged, they are highly resistant to the efforts of individual economic actors to change them – once networks become established, individual actors will experience lock-in effects.[30] Furthermore, under reasonable models of network growth, these topologies are self-reinforcing; as the pattern starts to become established, new nodes become overwhelmingly likely to reinforce rather than to undermine the existing unequal pattern of distribution.

---

[28] See Herbert A. Simon, "On a Class of Skew Distribution Functions," *Biometrika*, Vol. 42, No. 3/4 (1955), pp.425-440, Albert-László Barabási and Réka Albert. "Emergence of Scaling in Random Networks," *Science* Vol. 286, No. 5439 (1999), pp. 509-512.

[29] Ranjay Gulati, "Network Location and Learning: The Influence of Network Resources and Firm Capabilities on Alliance Formation." *Strategic Management Journal* Vol. 20, no. 5 (1999), pp. 397-420; Stephen P. Borgatti and Rob Cross. "A Relational View of Information Seeking and Learning in social networks." *Management Science* Vol. 49, no. 4 (2003), pp. 432-445.

[30] Brian W. Arthur, "Competing Technologies, Increasing Returns, and Lock-In by Historical Events," *The Economic Journal* Vol. 99, No. 394 (1989), pp. 116-131, Paul A. David, "Clio and the Economics of QWERTY," *The American Economic Review* Vol. 75, No. 2 (1985): 332-337.

Nor are these just abstract theoretical claims. They appear to describe many global economic networks.[31] Even when global networks largely came into being through entirely decentralized processes, they have come to display high skewness in the distribution of degree.[32] More plainly put, some nodes in these networks are far better connected than others. Studies of trade and banking show that the U.S. and the U.K. are exceptionally highly connected nodes in global financial networks. [33] It is increasingly difficult to map the network relations of the Internet for technical reasons, yet there is good reason to believe that the Internet displays a similar skew towards nodes in advanced industrial democracies such as the U.S. and (to a lesser extent) the U.K.[34]

All this activity is driven by a primarily economic logic. In a networked world, businesses often operate in a context where there are increasing returns to scale, network effects, or some combination thereof. These effects push markets toward winner-take-all equilibria in which only one or a few businesses have the lion's share of relationships with end users and, hence, profits and power. Even where networks are run by non profit actors, there are strong

---

[31] Thomas Oatley, W. Kindred Winecoff, Andrew Pennock, and Sarah Bauerle Danzman. "The Political Economy of Global Finance: A Network Model," *Perspectives on Politics* Vol. 11, No. 1 (2013), pp.133-153, Oatley, Thomas, *A Political Economy of American Hegemony*

[32] Réka Albert, Hawoong Jeong, and Albert-László Barabási. "Internet: Diameter of the World-Wide Web," *Nature* Vol. 401, No. 6749 (1999), 130-131, Stefania Vitali, James B. Glattfelder, and Stefano Battiston, "The Network of Global Corporate Control," *PloS One* Vol. 6, No. 10 (2011), pp. e25995, Camelia Miniou, and Javier A. Reyes. "A Network Analysis of Global Banking: 1978–2010," *Journal of Financial Stability* Vol. 9, No. 2 (2013), pp.168-184.

[33] On trade, see Giorgio Faviolo, Javier Reyes, and Stefano Schiavo, "World-Trade Web: Topological Properties, Dynamics, and Evolution," *Physical Review E* Vol. 79, No. 3 (2009), pp. 036115-1-19, Luca De Benedictis and Lucia Tajoli, "The World Trade Network," *The World Economy* Vol. 34, No. 8 (2011), pp. 1417-1454. On finance, see Thomas Oatley et al., "The Political Economy of Global Finance," William Kindred Winecoff, "Structural Power and the Global Financial Crisis: A Network Analytical Approach," *Business and Politics* Vol. 17, No. 3 (2015), pp. 495-525.

[34] Soon-Hyung, Yook, Hawoong Jeong, and Albert-László Barabási. "Modeling the Internet's Large-Scale Topology," *Proceedings of the National Academy of Sciences* Vol. 99, No. 21 (2002), pp. 13382-13386.

imperatives toward network structures in which most or even nearly all market actors work through a specific organization, allowing them to take advantage of the lower transaction costs associated with centralized communications architectures.

Once established, these centralized network structures are hard for outsiders to challenge, not least because they have focal power; challengers not only have to demonstrate that they have a better approach, but need to coordinate a significant number of actors to defect from the existing model or organization and converge towards a different one.

For example, Facebook's business model is centered on monetizing individuals' social networks through targeted advertisement and other means. It has been able to resist challengers with ostensibly better or less privacy-invasive products, because it is relatively costly for an individual, or even a medium-sized group, to move to a different service unless they know that everyone else is doing the same thing. Google similarly leverages the benefits of search and advertising data.[35] Large international financial institutions such as Citibank, security settlement systems such as Euroclear, consumer credit payment systems such as Visa/Mastercard, financial clearing houses such as the Clearing House Interbank Payments System, and financial messaging services such as SWIFT have become crucial intermediaries in global financial networks, acting as middlemen across an enormous number and variety of specific transactions. All these actors play key roles in their various architectures, coordinating and brokering numerous specific

[35] On power relations in the platform economy, see Lina M. Khan, "The Ideological Roots of America's Market Power Problem," *Yale Law Journal Forum* (2018), https://www.yalelawjournal.org/pdf/Khan_xktx9xrh.pdf, Lina M. Khan, "Amazon's Anti-Trust Paradox," *Yale Law Journal* (2017), Vol. 126, pp.710-805.

relationships, benefiting from efficiencies of scale and in some cases from the unique access to information that their brokerage position supplies.[36]

Notably, the most central nodes are not randomly distributed across the world but are typically territorially concentrated in the advanced industrial economies, and the United States in particular. This distribution reflects a combination of the rich-get-richer effects common in network analysis and the particular timing of the most recent wave of globalization, which coincided with US and Western domination of relevant innovation cycles.

In short, globalization has generated a new set of structural forces. Economic actors' myriad activities create self-reinforcing network topologies, in which some economic intermediaries – nodes – are centrally located with very high degree, and the vast majority of other nodes are dependent on them. Once these topologies become established, it is difficult for economic actors to change or substantially displace them.

New Forms of Network Power: Panopticons and Chokepoints

The asymmetric networks that make up much of the structure of a globalized world were not constructed as tools of statecraft. They typically reflect the incentives of businesses to create monopolies or semi-monopolies, increasing returns to scale in certain markets, "rich get richer" mechanisms of network attachment and the efficiencies available to more centralized communications networks. By building centralized networks, market actors inadvertently provide states, which are concerned with political as well as economic considerations, with the necessary levers to extend their influence across borders. Thus, structures that were generated by

[36] Judge, "Intermediary Influence"; Natasha Tusikov, *Chokepoints: Global Private Regulation on the Internet* (Berkeley: University of California Press, 2016).

market actors in pursuit of efficiency and market power can be put to quite different purposes by states.

Here, we differentiate our account of power from two related but distinct sources of power that may result from economic interdependence. The first is market power. Although often underspecified, research on market power emphasizes the aggregate economic potential (measured in a variety of different ways ranging from the domestic consumer-base to aggregate gross domestic product) of a country. States with large economic markets can leverage market access for strategic ends. National economic capabilities, then, produce power resources.[37] The second source of power, which dates back to the pioneering work of Keohane and Nye and has been most thoroughly examined in the case of trade, involves bilateral dependence. States that rely on a particular good from another state and lack a substitute supplier may be sensitive to shocks or manipulation.[38]

Market size and bilateral economic interactions are important, but they are far from exhaustive of the structural transformations wreaked by globalization. Global economic networks have distinct consequences that go far beyond states' unilateral decisions either to allow or deny market access, or to impose bilateral pressure. They allow some states to weaponize interdependence on the level of the network itself. Specifically, they enable two

---

[37] Shambaugh, George E. "Dominance, Dependence, and Political Power: Tethering Technology in the 1980s and Today." *International Studies Quarterly* 40.4 (1996): 559-588; Simmons, Beth A. "The International Politics of Harmonization: The Case of Capital Market Regulation." *International Organization* 55.3 (2001): 589-620; Daniel Drezner, *All Politics is Global*. Princeton: Princeton University Press. 2007. Kalyanpur, Nikhil, and Abraham L. Newman. "Mobilizing Market Power: Jurisdictional Expansion as Economic Statecraft." *International Organization* 73. 1 (2019): 1-34.

[38] Keohane and Nye, *Power and Interdependence,* Joanne Gowa, "Bipolarity, Multipolarity, and Free Trade,"; Brian M. Pollins, "Does Trade Still Follow the Flag?,"; John R. Oneal, Frances H. Oneal, Zeev Maoz, and Bruce Russett. "The Liberal Peace: Interdependence, Democracy, and International Conflict, 1950-85,"; Copeland, *Economic Interdependence and War*.

forms of weaponization. The first weaponizes the ability to glean critical knowledge from information flows, which we label the "panopticon effect." Jeremy Bentham's conception of the Panopticon was precisely an architectural arrangement in which one or a few central actors could readily observe the activities of others. States that have physical access to or jurisdiction over hub nodes can use this influence to obtain information passing through the hubs. Because hubs are crucial intermediaries in decentralized communications structures, it becomes difficult – or even effectively impossible – for other actors to avoid these hubs while communicating.

This phenomenon existed in earlier periods of globalization as it did today. As Harold James describes it, "in the first era of globalization, expanding trade, capital and labour flows all tied economies together in what appeared to be an increasing and probably irreversible network," centered on the "commercial infrastructure provided by Britain," and in particular the financial infrastructure of the City of London.[39] As James notes:

> the fact that Britain was the hub of trade finance and insurance gave its military planners, and its political-decision makers, a unique insight into how and where global flows of strategic goods went, and how those flows might be interrupted.[40]

As technology has developed, the ability of states to glean information about the activities of their adversaries (or third parties on whom their adversaries depend) has correspondingly become more sophisticated. The reliance of financial institutions on readily searchable archives of records converts bank branches and Internet terminals into valuable

[39] P.43, Harold James, "Cosmos, Chaos: Finance, Power and Conflict," *International Affairs* Vol. 90, No. 1 (2015), pp.37-57.
[40] P.54, Harold James, "Cosmos, Chaos."

sources of information. New technologies such as cell phones become active sensors that can be tapped into by appropriate technologies. Under the panopticon effect, states' direct surveillance abilities may be radically outstripped by their capacity to tap into the information-gathering and generating activities of networks of private actors.

Such information offers privileged states a key window into the activity of adversaries, partly compensating for the weak information environment that is otherwise characteristic of global politics. As a result, states with access to the panopticon effect have an informational advantage in understanding adversaries' intentions and tactics. This information offers those states with access to the hub a strategic advantage in their effort to counter the specific moves of their targets, conduct negotiations, or create political frames.

The second channel works through what we label the "chokepoint effect," and involves privileged states' capacity to limit or penalize use of hubs by third parties (e.g. other states or private actors). Because hubs offer extraordinary efficiency benefits, and because it is extremely difficult to circumvent them, states that can control hubs have considerable coercive power, and states or other actors that are denied access to hubs can suffer very substantial consequences. Again, there is some historical precedent for this phenomenon. Nicholas Lambert describes how the U.K. enjoyed a near monopoly over the communications infrastructure associated with international trade in the period before World War I, and developed extensive plans to use this monopoly to disrupt the economies of their adversaries, weaponizing the global trading system.[41]

[41] Nicholas Lambert. *Planning Armageddon: British Economic Warfare and the First World War*. Harvard University Press, 2012.

As Heidi Tworek argues, Germany responded to the U.K. stranglehold on submarine communication cables by trying to develop new wireless technologies.[42]

States may use a range of tools to achieve chokepoint effects, including those described in the existing literature on how statecraft, credibility, the ability to involve allies, and other such factors shape the relative success or failure of extraterritorial coercive policies.[43] In some cases, states have sole jurisdiction over the key hub or hubs, which offers them the legal authority to regulate issues of market use. In others, the hubs may be scattered across two or more jurisdictions, obliging states to work together to exploit the benefits of coercion. Our account emphasizes the crucial importance of the network structures within which all of these coercive efforts take place. Where there are one or a few hubs, it becomes far easier for actors in control of these nodes to block or hamper access to the entire network.

We explain variation in state strategies as a function of the structural topography of the network combined with domestic institutions and norms of the states attempting to make use of the network structures. First, only those states that have physical or legal jurisdiction over hub nodes will be able properly to exploit the benefits of weaponized interdependence. As we have already noted, the network hubs of globalization are not scattered at random across the world. Instead, they are disproportionally located in the advanced industrial countries, in particular the United States, which has led technological and market innovation in the most recent round of economic globalization. This geographic skew effectively means that only the U.S. and a couple

---

[42] Heidi Tworek. *News from Germany: The Competition to Control World Communications, 1900-1945.* Harvard University Press, 2019.

[43] Kaczmarek, Sarah C., and Abraham L. Newman. "The Long Arm of the law: Extraterritoriality and the National Implementation of Foreign Bribery Legislation." *International Organization* 65, no. 4 (2011), pp. 745-770; Raustiala, Kal. *Does the Constitution Follow the Flag?: The Evolution of Territoriality in American Law*. Oxford University Press, 2011; Putnam, Tonya L. *Courts Without Borders: Law, Politics, and US Extraterritoriality*. Cambridge University Press, 2016.

of other key states and state like entities (most notably, the E.U. and, increasingly, China) enjoy the benefits of weaponized interdependence, although others may still be able to play a disruptive role.

Second, there will be variation across the national institutional structures associated with different issue areas. If states are to exploit hubs, they require appropriate legal and regulatory institutions. Depending on domestic configurations of power and state-society relations, they may lack coercive capacity, or alternatively, may be able to prosecute strategies only based on panopticon effects rather than chokepoints, or vice versa. The literature on regulatory capacity, for example, demonstrates that the United States is not uniformly positioned to control market access.[44] In some areas, it has weak or decentralized regulatory institutions, or would face powerful domestic pushback. In such cases, states may find themselves structurally positioned to shape hub behavior but lack the institutional resources to exploit either or both the panopticon or chokepoint effects.

In other domains, national laws and norms may constrains states from engaging in certain kinds of weaponization. Privacy laws in the European Union, for example, limit the amount of data that may be collected or stored by commercial internet providers.[45] These institutions, which were adopted just as decentralized market processes generated new commercial networks of data exchange, mean that it is more difficult for many European governments to directly exploit

---

[44] David Bach and Abraham L. Newman. "The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence." *Journal of European Public Policy* Vol. 14, No. 6 (2007), pp. 827-846; Posner, Elliot. "Making Rules for Global Finance: Transatlantic Regulatory Cooperation at the Turn of the Millennium." *International Organization* Vol. 63, No. 4 (2009), pp. 665-699; Tim Büthe and Walter Mattli. *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton, NJ: Princeton University Press, 2011); Nikhil Kalyanpur and Abraham Newman, "Mobilizing Market Power".

[45] Abraham L. Newman. *Protectors of Privacy: Regulating Personal Information in the Global Economy* (Ithaca: Cornell University Press, 2008).

panopticon effects. As history demonstrates, domestic institutions may change in response to new perceived external threats, but they may also be sticky, because domestic actors may fear that the new capacities will be turned against them as well as foreign adversaries.[46] Domestic institutions are usually themselves the product of intense internal political battles, so that they cannot costlessly be transformed to confront new international challenges.

The central expectation of our argument is that states' variable ability to employ these forms of coercion will depend on the combination of the structure of the underlying network and the domestic institutions of the states attempting to use them. States that have jurisdictional control over network hubs and enjoy sufficient institutional capacity will be able to deploy both panopticon and chokepoint effects. Variation in domestic institutions in terms of capacity and key norms may limit their ability to use these coercive tools even when they have territorial or jurisdictional claims over hubs. Where control over key hubs is spread across a small number of states, these states may need to coordinate with one another to exploit weaponized interdependence. States that lack access to, or control over, network hubs will not be able to exert such forms of coercion.

In the succeeding sections, we provide a plausibility probe for our argument. We present two analytic narratives covering different core policy domains of globalization – financial and international data flows. In each domain, we demonstrate how a similar structural logic developed, as highly asymmetric networks emerged, in which a few hubs played a key role. In contrast to liberal approaches, we show how states – most particularly the U.S. – were able to take advantage of these network structures, to exploit panopticon effects or chokepoint effects.

---

[46] Farrell, Henry, and Abraham L. Newman. "Making Global Markets: Historical Institutionalism in International Political Economy." *Review of International Political Economy* 17, no. 4 (2010): 609-638; Farrell, Henry, and Abraham L. Newman. "Domestic Institutions Beyond the Nation-State: Charting the New Interdependence Approach." *World Politics* 66, no. 2 (2014): 331-363.

Importantly, our cases offer variation in the ability of the U.S. to deploy these strategies, distinguishing our argument from more conventional market power or bilateral vulnerability accounts.

The Rise of Network Inequality

Although globalization is often characterized as involving complexity and fragmentation, this section demonstrates how strong systematic inequalities have emerged in two issue areas – finance and information. In particular, these narratives demonstrate how market actors created institutions and technologies to overcome the transaction costs associated with decentralized markets and, in doing so, generated potential sites of control.

Global Finance and SWIFT's Centrality

To manage billions of daily transactions and trades, global finance relies on a much smaller set of backroom arrangements to facilitate capital flows – so-called payment systems. Businesses and banks depend on these payment systems to move funds from one entity to another. A key component of the payment system, then, is reliable and secure communication between financial institutions regarding the multitude of transactions that occur globally on any given day.

Since the 1970s, inter-bank communication has been provided by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[47] For much of the post-World

[47] Our history of SWIFT in this section relies extensively on Susan V. Scott and Markos Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community* (London: Routledge, 2014). SWIFT is remarkably understudied by international security scholars, considering its empirical importance to sanctions. For a key exception, see Erik Jones, and Andrew Whitworth. "The Unintended Consequences of European Sanctions on Russia," *Survival* Vol. 56, No. 5 (2014), pp. 21-30. For discussions of SWIFT in the EU-US relationship, see

War II period, only a few transnational banks engaged in cross-border transactions. Those that did had to rely on the public telegram and telex systems, which were operated by national telecommunications providers. These systems proved both slow and insecure. These inefficiencies led financial actors to create a number of competing platforms for interbank communication in the 1970s. Most notably, the First National City Bank of New York (FNCB later renamed Citibank) developed a proprietary system known as Machine Readable Telegraphic Input (MARTI), which the company hoped to disseminate and profit from.

This system gave a big push to European banks and US competitors of FNCB, which worried about what might happen if they became dependent on MARTI. The result was that a small group of European and US banks cooperated in building a messaging system that could replace the public providers and speed up the payment process. SWIFT opened its doors in 1973 and sent its first message in 1977.

The main objective of the organization was to create a system for transferring payment instructions between entities engaged in a financial transaction including banks, settlement institutions, and even central banks. SWIFT plays a critical role in authorizing transactions, authenticating parties, and recording exchanges. It is a cooperative run by representatives from the different financial institutions involved. SWIFT's headquarters are located near Brussels, Belgium, to sidestep the emerging rivalry between New York and London as the hubs of global banking.

For much of the 1970s, it was unclear if SWIFT would succeed. The organization had to develop a new secure messaging system that could efficiently transfer tremendous amounts of

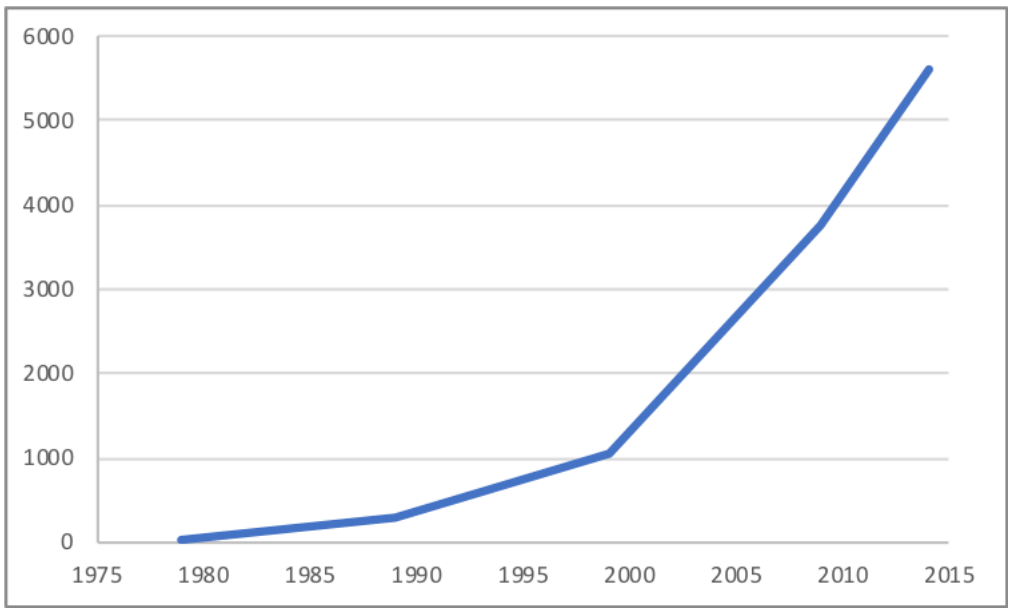
---

Marieke De Goede, "The SWIFT Affair and the Global Politics of European Security," *Journal of Common Market Studies* Vol. 50, no. 2 (2012), pp. 214-230; Henry Farrell and Abraham Newman, "The New Politics of Interdependence: Cross-National Layering in Trans-Atlantic Regulatory Disputes," *Comparative Political Studies*, Vol. 48, No. 4 (2015), pp. 497-526.

data and beat competitors such as MARTI. In 1977, it was used in 22 countries by roughly 500 firms with an annual traffic of approximately 3000 messages. By 2016, it had become the dominant provider serving more than 200 countries and some 11,000 financial institutions, carrying over 6.5 billion messages annually. As Susan Scott and Markos Zachariadis note, "Founded to create efficiencies by replacing telegram and telex (or 'wires') for international payments, SWIFT now forms a core part of the financial services infrastructure."[48] This network effect was an accidental rather than an intended outcome. Those involved in the original SWIFT project during the 1970s were solely focused on "creating an entity, a closed society, to bind members together in an organizational form that would employ standards designed to create efficiencies on transactions between the member banks."[49]

Figure 1. Annual SWIFT Messages in Millions*

[48] P.1, Susan V. Scott and Markos Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication*.
[49] P.107, Scott and Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication.*



* The acronym SWIFT stands for Society for Worldwide Interbank Financial Telecommunications.

Eventually, the organization's dominance over financial messaging led to monopoly regulation by the Commission of the European Union. La Poste (the deregulated Postes, Télégraphes et Téléphones of France) sought access to the SWIFT network as part of its banking operations, and SWIFT denied the request on the grounds that La Poste was not a traditional banking institution. The European Commission ruled in 1997 that SWIFT's "dominant position…since it is the only operator on the international networks for transferring payment messages" meant that it was a quasi-utility and had to follow an open access model. As a result, even more financial institutions began to use and become dependent on the SWIFT system. The more banks that used SWIFT, the more it created measurable network benefits for its members,

and the less likely member banks were to defect.[50] By the turn of the millennium, nearly all major global financial institutions used the SWIFT system to process their transactions.

The Internet – All roads lead through Northern Virginia

Like financial messaging, the Internet is often described as a decentralized network, in which digital packets effortlessly route around blockages. It too had its origins in technical discussions, that ran parallel to politicized global debates. In the early 1970s, countries in the developing world pushed for a "New World Communication and Information Order"

> "that would inter alia require the licensing of journalists, enhanced abilities for governments to keep out unwanted transmissions of news and other information, and a 'balanced' flow of information between the global North and South."[51]

This push from developing countries led to discussions in the Organization for Economic Cooperation and Development (OECD) about whether transborder data flows posed a problem for national sovereignty.[52] The US government and US businesses looked to divert this debate, ensuring that the OECD Declaration on Transborder Data Flows in 1985 called on governments

[50] Susan V. Scott, John Van Reenen and Markos Zachariadis, *The Long-Term Effect of Digital Innovation on Bank Performance: An Empirical Study of SWIFT Adoption in Financial Services* Discussion Paper No. 992 (London: London School of Economics Center for Economic Performance 2017).
[51] P.5, William Drake, *Background Paper: WEF Workshop on Data Localization and Barriers to Transborder Data Flows*. http://www.academia.edu/34713765/Drake_William_J._2016._Background_Paper_WEF_Workshop_on_Data_Localization_and_Barriers_to_Transborder_Data_Flows.pdf.
[52] IBID.

"to avoid the creation of unjustified barriers to the international exchange of data and information."[53] Proposals for a wide-reaching set of international institutions fell by the wayside. Instead, the OECD principles were nonbinding and focused on privacy, where the US and EU member states came to loose agreement in principle but not practice. While these disagreements were taking place, technical experts, who were mainly interested in the best ways of sharing scarce computer resources within the US research and military establishment, developed technical proposals for "packet switching" into the Transmission Control Protocol/Internet Protocol (TCP/IP protocol), which, in modified form, remain the cornerstone of the internet today. The internet spread internationally, but primarily within a specialized technical community, so that, for example, national top-level domain names were effectively allocated by a single individual, Jon Postel, to persons or organizations he deemed trustworthy.

When the internet came to public prominence in the early 1990s, it initially seemed as though it might provide a technology that was innately resistant to centralization. Authorities and political actors including US President Bill Clinton believed that it was effectively invulnerable to central control.[54] In contrast to "centralized" networks such as the then existing phone system, where different phones connected through a central switchboard, the Internet was conceived as a "distributed" network, where there was a multiplicity of ties between different nodes, and no node was innately more important than any other.[55] The TCP/IP protocol allowed servers to speedily identify blockages in the system and find alternative routes for information. In such a

---

[53] P.51, William J. Drake, "Introduction," William J. Drake and Ernest J. Wilson (eds), *Governing Global Electronic Networks: International Perspectives on Policy and Power* (Cambridge MA: The MIT Press, 2008).

[54] William J. Clinton, *Remarks at the Paul H. Nitze School of Advanced International Studies*, Washington DC, Johns Hopkins SAIS, March 8, 2000. http://www.presidency.ucsb.edu/ws/?pid=87714.

[55] On the theory of distributed networks, see Paul Baran, "On Distributed Communications Networks," IEEE Transactions on Communications Systems Vol. 12, No. 1 (1964), pp.1-9.

system, government control seemed very difficult – as the prominent activist John Gilmore put it, the "Net interprets censorship as damage, and routes around it."[56] This resistance to blockages led some online libertarians to forecast the withering of the state and a new age of human freedom.[57]

Contradicting these heady prognoses, the underlying architecture of the Internet became increasingly centralized over time.[58] Some hubs and interconnections between these hubs became far more important than others. States increasingly were able to impose controls on traffic entering and leaving their country, while censoring or controlling many ordinary uses of the Internet.[59] The most important infrastructural elements of the Internet are the fiber optic cables that provide service between the continents. These cables are far more efficient than competing channels such as satellite or legacy telephone wires. They are also geographically fixed. 97% of intercontinental Internet traffic travels across roughly 300 cables.[60] The importance of these central communication nodes became painfully clear in 2008, when a ship's anchor severed two such cables (FLAG Europe Asia and SEA-ME-WE-4) off the cost of Egypt

[56] Philip Elmer-Dewitt, "First Nation in Cyberspace," *Time Magazine*, December 6, 1993. http://content.time.com/time/magazine/article/0,9171,979768,00.html.
[57] John Perry Barlow, "A Declaration of the Independence of Cyberspace." *The Humanist* Vol. 56, No. 3 (1996), p 18.
[58] Albert, Jeong, and Barabási. "Internet: Diameter of the World-Wide Web."
[59] Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006), Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Janice Gross Stein. *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: The MIT Press, 2008), Adam Segal, *The Hacked World* Order (New York, NY: Public Affairs 2017), Joshua A. Tucker, Yannis Theocharis, Margaret E. Roberts, and Pablo Barbera (2017), "From Liberation to Turmoil: Social Media and Democracy," *Journal of Democracy*, Vol. 28, No.4, pp.46-59.
[60] Asia-Pacific Economic Cooperation (APEC) Secretariat, *Economic Impact of Submarine Cable Disruptions,* Asia-Pacific Economic Cooperation, February 2013.

and shut down much of the Internet in the Middle East and South Asia. The recurrence of such problems has led to concerns about vulnerability to sabotage.[61]

The increasing complexity and size of the modern Internet threatens to slow connection speeds. In response, internet exchange points have emerged, which facilitate communication across service providers and infrastructure backbones.[62] These internet exchanges are often located in major cities and channel the majority of domestic internet traffic in the United States and Europe; they also support peer linkages between the different global networks that allow the Internet to function. Once again, this means that a substantial amount of traffic travels through a few key nodes.

Network economies have similarly led to a centralization of the e-commerce economy, as both network effects and new kinds of increasing returns to scale cemented the global dominance of a very small number of e-commerce companies. This dominance is in part thanks to US government policy. The US believed that to the greatest extent possible, data governance should involve the free flow of content across borders (except, of course, where this interfered with the intellectual property or other vital interests of US corporations). It should furthermore be based primarily on self-regulation, looking to business cooperation and market structures to regulate their relations with consumers.[63]

This emphasis on self-regulation and individual choice gave private firms a great deal of freedom to set their own rules. In the 1990s, Clinton administration officials, led by Ira

---

[61] APEC Secretariat, *Economic Impact of Submarine Cable Disruptions.*
[62] See Patrick S. Ryan and Jason Gerson. "A Primer on Internet Exchange Points for Policymakers and Non-Engineers," *Social Science Research Network* (2012). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2128103, Kuai Xu, Zhenhai Duan, Zhi-Li Zhang, and Jaideep Chandrashekar, "On Properties of Internet Exchange Points and Their impact on AS Topology and Relationship." In *International Conference on Research in Networking*, pp. 284-295. Springer, Berlin, Heidelberg, 2004.
[63] Author Interview with Ira Magaziner, New York, September 21, 2000.

Magaziner, crafted a "Framework for Global Electronic Commerce" that was intended to shape the emerging international debate so as to push back against government regulation and, instead, favor self-regulatory approaches.[64] The US government scotched plans by Postel to set up a global institution to regulate the Internet with the help of the Internet Society and the UN's International Telecommunications Union, threatening him with criminal sanctions if he did not back down.[65]

Instead, it handed authority over domain names to a private nonprofit corporation under Californian law, the Internet Corporation for Assigned Names and Numbers (ICANN), which would work with for-profit entities to manage the technical aspects of coordination.[66] ICANN's ultimate authority stemmed from a contract with the Department of Commerce – this provided the U.S. government with a controversial implicit veto. Importantly, however, ICANN was designed according to a "stakeholder" model, under which private actors would take the lead in shaping its deliberations. The US veto was primarily intended as a backstop against other states or international organizations wresting ICANN away from the private sector, rather than a calibrated tool for institutional interference.

Self-regulation and individual choice were also the organizing principles for US domestic regulations. These principles were laid out in legislation including, most importantly, Section 230 of the 1996 Communications Decency Act – which protected e-commerce firms from "intermediary liability" for content put up by others.[67] This section was intended for a specific

---

[64] United States White House Office, *A Framework for Global Electronic Commerce* (Washington, DC: White House, 1997).
[65] Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge MA: The MIT Press 2009).
[66] Mueller, *Ruling the Root.*
[67] Jack M. Balkin, "The Future of Free Expression in a Digital Age," *Pepperdine Law Review* Vol. 36 (2008), pp.427-444.

and relatively narrow purpose – to provide businesses with safe harbor against legal actions aimed at content posted by users. It ended up inadvertently supporting a new business model, in which e-commerce firms, rather than providing content themselves, would rely on their users to provide the content for them. They could then make their profits by acting as an intermediary between those users, analyzing their behavior, and offering targeted advertising services to their actual customers, people who wanted to sell products to the users leaving data trails behind them.

Section 230, together with network effects, led to the rapid domination of a small number of e-commerce and online companies. Companies such as Facebook and YouTube (owned by Google and then by Alphabet) were able to use the lack of intermediary liability to rapidly scale up, allowing enormous numbers of users to share content, without any need for companies to edit or inspect that content, except when they were informed of intellectual property violations. The result was a business model based on algorithms rather than employees.[68] Google could similarly take advantage of the lack of intermediary liability, while expanding into new services. It reaped the benefits of a feedback loop in which its users passively provided data, which could be categorized using machine learning techniques both to sell space to advertisers and to further improve Google services. Amazon, too, swiftly branched out, selling not only physical products, but cloud services, and acting as an intermediary across a wide variety of markets.

All these firms built themselves effective near monopolies. Facebook – once it had become established – was more or less impossible for competitors to displace, because its users had little incentive to migrate to a new system, and Facebook could buy and integrate potential new competitors long before they could become real threats. Google's data dominance provided

[68] See more generally, Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

the company with a nearly impregnable position, while Amazon's relentless growth into new marketplaces provided it with irresistible economies of scale.[69]

Although China has excluded these companies and developed domestic competitors, it has done so only by leveraging state power in ways that are far harder for small states and liberal democracies. As a result, a huge fraction of global data traffic is channeled through the servers of a handful of companies, which sit in the United States. Key aspects of the domain name system are run by ICANN, which provided some privileged actors with levers for achieving political outcomes.[70] In addition, as ever more online services move to cloud architectures, which store customer data and processing power in online data centers, cloud providers have emerged as central hubs.[71] One estimate, for example, suggests that 70 percent of global web traffic goes through Amazon Web Services in Northern Virginia (which had become established as a hub location decades earlier thanks to America Online).[72] Thus, transcontinental fiber optic cables, internet exchanges, monopoly service providers and geographically concentrated data centers have all helped build a grossly asymmetric network, in which communications, rather than being broadly distributed, travel through key hubs, which are differentially concentrated in the U.S, and channel the vast majority of global data exchanges.

Weaponizing the Hubs

[69] Khan, "Amazon's Anti-Trust Paradox."
[70] See Laura DeNardis, "Hidden Levers of Internet Control," *Information, Communication and Society*, Vol. 15, No. 5, pp. 720-738; Tusikov, *Chokepoints*.
[71] Bruce Schneier, "Censorship in the Age of Large Cloud Providers," *Lawfare*, June 7 2018. https://lawfareblog.com/censorship-age-large-cloud-providers.
[72] Benjamin Freed, "70 Percent of the World's Web Traffic Flows through Loudoun County," *Washingtonian*, September 14, 2016.

With the rise of these central hubs across financial messaging and online comminucation, states (and in particular the U.S. and the E.U.) began to understand that they could exploit network properties to weaponize interdependence. In what follows, we use the case evidence to demonstrate the two forms of network power – panopticon and chokepoint effects – and explain variation in their use. In particular, the case of financial messaging underscores the importance of institutional capacity and differences between the US and Europe in their ability to employ these strategies. The case of the Internet underscores how domestic institutions and norms constrain the behavior of the United States even when it has physical and legal jurisdiction over key hubs.

SWIFT, Counterterrorism and Nonproliferation

SWIFT demonstrates how both the panopticon and chokepoint effects can work in global networks. Because SWIFT is central to the international payment system, it both provided data about the vast majority of global financial transactions and allowed these transactions to take place. For the last twenty-five years, key states, most importantly the US, have gradually transformed the repository of transfers into a surveillance asset and financial sector dependence into a tool of asymmetric interdependence.

Although the terrorist attacks of September 11th 2001, were a crucial moment in global surveillance politics, governments began considering SWIFT's potential much earlier. The Financial Action Task Force (FATF), a core global governance body focused on anti-money laundering, focused initially on organized crime and drug trafficking, and approached SWIFT in 1992.[73] FATF hoped to gain access to SWIFT records so as to track down illicit activity. At this

[73] On FATF, see Julia Morse, "Blacklists, Market Enforcement, and the Global Regime to Combat Terrorist Financing," *International Organization* (forthcoming), Eleni Tsingou, "Global Financial Governance and the Developing Anti-Money Laundering Regime: What Lessons for

point, SWIFT realized the peril of the economic efficiencies that it itself had created. As Lenny Schrank, a former chief officer of SWIFT, later reflected, "This was when we first began to think the unthinkable: that maybe we have some data that authorities would want, that SWIFT data would be revealed…and what to do about it…no one thought about terrorism at that time."[74] SWIFT refused the request, claiming that it could not provide information to public authorities and that such requests had to be directed to banks and other financial institutions engaged in the transaction. The organization claimed that it was a communications carrier much like a telephone operator rather than a data processor and thus should be immune to government monitoring.

SWIFT resisted government pressure for much of the 1990s, but succumbed after the September 11 attacks.[75] In the wake of the attacks, the U.S. Treasury began to examine ways to use the global financial system to curtail terrorist financing, targeting the terrorist money supply, and concluded that it could lawfully issue enforceable subpoenas against SWIFT to compel it to provide financial data. The Treasury initiative became known as the Terrorist Finance Tracking Program (TFTP) and targeted SWIFT as a key source of data. It was especially hard for SWIFT to resist Treasury demands, because the organization maintained a mirror data center containing its records in Virginia. In the years that followed, SWIFT secretly served as a global eye for the US fight against terrorism, with the Treasury using the SWIFT system to monitor and investigate illicit activity.[76] As Juan Zarate, a former treasury department official, explained: "Access to

---

International Political Economy?," *International Politics*, Vol. 47, No.6 (2010), pp.617-637, Anne L. Clunan, "The Fight Against Terrorist Financing," *Political Science Quarterly* Vol 121, No. 4 (2006-2007), pp. 569-596.

[74] P. 128, Scott and Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication.*

[75] See Caytas, "Weaponizing Finance", pp.441-475 for an excellent overview of both SWIFT and the dollar clearing system.

[76] Eric Lichtblau and James Risen, "Bank Data is Sifted by US in Secret to Block Terror," *New York Times*, June 23 (2006).

SWIFT data would give the US government a method of uncovering never-before-seen financial links, information that could unlock important clues to the next plot or allow an entire support network to be exposed and disrupted."[77]

The SWIFT data became the Rosetta stone for US counter-terrorism operations as it shed light on the complex networks of terrorist financing.[78] The government used the data as a key forensic tool to identify terrorist operations, co-conspirators and planning. This effort became so central to US and European counterterrorism operations that when it was challenged by European actors worried about civil liberties, the US government employed top officials including Secretary of State Hillary Clinton and Secretary of the Treasury Timothy Geithner to defend and demand the continuation of the program. [79] As one EU foreign minister concluded, "They pulled out all the moral and political stops."[80] After a joint review of the program, the European Commission argued: "The Commission is of the view that the TFTP remains an important and efficient instrument contributing to the fight against terrorism and its financing in the United States, the EU and elsewhere."[81] Despite initial public protests, the dominant coalition

[77] P. 50, Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (London, UK: Hachette 2013).
[78] Lichtblau and Risen, "Bank Data is Sifted."
[79] For detailed discussion, see Henry Farrell and Abraham Newman, *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security* (Princeton, NJ: Princeton University Press 2019).
[80] Hans-Jürgen Schlamp, "EU to Allow US Access to Bank Transaction Data," *Spiegel Online*, November 27 (2009). https://www.spiegel.de/international/europe/spying-on-terrorist-cash-flows-eu-to-allow-us-access-to-bank-transaction-data-a-663846.html (checked April 28, 2019).
[81] European Commission, *Joint Review Report of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the Untied States for the purposes of the Terrorist Finance Tracking Program*, SWD(2017) 17 final. European Commission: Brussels (2017).

in EU politics quietly approved of the U.S. use of SWIFT to create a financial data panopticon, so long as the U.S. was prepared to share the proceeds.[82]

U.S. and E.U. efforts to weaponize SWIFT were not limited to the panopticon effect. As Joanna Caytas notes: "The most vulnerable element of financial infrastructure is its payments system, both at a national (macro) level and on an institutional (micro) plane." [83] Caytas furthermore argued that "Disconnection from SWIFT access is, by any standard, the financial market equivalent of crossing the nuclear threshold, due to the vital importance of the embargoed services and near-complete lack of alternatives with comparable efficiency."[84]

As an example of the power of chokepoints, US and European policymakers used SWIFT to reinforce the sanctions regime against Iran. A group of prominent US policy-makers, led by Ambassadors Richard Holbrook and Dennis Ross, started a private campaign, known as United Against Nuclear Iran (UANI) in the 2000s, to ratchet up pressure on the Iranian regime. The group targeted SWIFT as complicit in assisting the Iranian regime and contributing to its economic health.[85] As per SWIFT's 2010 annual report, some nineteen Iranian banks as well as another twenty-five institutions relied on the messaging system.[86] In January 2012, UANI sent a letter to SWIFT arguing that "the global SWIFT system is used by Iran to finance its nuclear weapons program, to finance terrorist activities and to provide the financial support necessary to brutally repress its own people."[87]

---

[82] Farrell and Newman, "The New Politics of Interdependence."
[83] P. 449, Caytas, "Weaponizing Finance."
[84] P. 451, Caytas, "Weaponizing Finance."
[85] United Against Nuclear Iran, *SWIFT Campaign* (Washington DC: UANI 2012).
[86] SWIFT, *Annual Review 2010: Common Challenges, Unique Solutions*, SWIFT: Brussels (2010).
[87] UANI Letter to SWIFT, January 30, 2012. https://www.unitedagainstnucleariran.com/sites/default/files/IBR%20Correspondence/UANI_Let

This campaign had consequences in both the U.S. and Europe. On February 2, 2012, the US Senate Banking Committee adopted language that would have allowed the US government to sanction SWIFT if it continued to allow Iranian financial institutions to use the SWIFT system, pushing the administration to adopt a more pro-active stance.[88] The European Union followed up on this threat in March, motivated both by both US pressure and its own worries about Iran's nuclear program, and passed regulations that prohibited financial messaging services (e.g., SWIFT) from providing services to targeted institutions.[89]

The combination of E.U. and U.S. sanctions required SWIFT to cut Iranian banks out of its system. In 2012, the E.U's Council banned the provision of financial messaging services to Iran.[90] As Lazaro Campos, a former chief executive officer of SWIFT, concluded, "This EU decision forces SWIFT to take action. Disconnecting banks is an extraordinary and unprecedented step for SWIFT. It is a direct result of international and multilateral action to intensify financial sanctions against Iran."[91]

The Iranian regime quickly felt the consequences as its major financial institutions, including its central bank, found themselves locked out from the international payment system.

---

ter_to_SWIFT_013012.pdf; Jay Solomon and Adam Entous, "Banking Hub adds to Pressure on Iran," *Wall Street Journal*, February 4 (2012).

[88] Jay Solomon, *The Iran Wars: Spy Games, Bank Battles, and the Secret Deals that Reshaped the Middle East* (New York: Random House 2016).

[89] Agence France Presse, "US presses EU to close SWIFT network to Iran," February 16 (2012); Samuel Rubenfeld, "SWIFT to Comply with EU Ban on Blacklisted Entities," *Wall Street Journal*, March 15 (2018).

[90] Arnold, "The True Cost of Financial Sanctions."; Associated Press, "Iran cut off from Global Financial System," March 15 (2012).

[91] SWIFT press release, March 15 2012. https://www.unitedagainstnucleariran.com/index.php/swift.

As explained by a E.U. official at the time, "It is a very efficient measure…It can seriously cripple the banking sector in Iran."[92]

Unwinding the SWIFT measures became a key bargaining point in the negotiations over Iran's nuclear program.[93] During the negotiations with the United Nations Security Council's five permanent members, plus Germany, Iranian Foreign Minister Javad Zarif, made it clear that lifting the SWIFT ban was a top priority. "The deal will be made or broken," he said during an interview in July 2015, "[depending] on whether the United States wants to lift the sanctions or keep them." [94] Accordingly, a lifting of the SWIFT measures was a key part of the eventual Iran deal.

Notably, the SWIFT measures were a result of joint pressure from both of the jurisdictions to which it was substantially exposed to. Had the U.S. not imposed pressure, it is unlikely that the E.U. would have been able to act on its own; as Caytas notes, the E.U.'s fragmented internal decisionmaking structures and lack of supple institutions undermines its ability to weaponize finance.[95] Equally, however, the U.S. might have had difficulties in acting unilaterally in the face of concerted E.U. opposition, given SWIFT's primary location in Europe.

More recently the politics of the SWIFT chokepoint have become more complex. As the U.S. backed out of the JCPOA, it threatened to reimpose SWIFT restrictions on Iran, while the European Union resisted the re-weaponization of SWIFT.[96] SWIFT responded to the threat of

---

[92] Rick Gladstone and Stephen Castle, "Global Network Expels as Many as 30 of Iran's Banks in Move to Isolate its Economy," *New York Times*, March 15 (2012).
[93] Zarate, *Treasury's War*.
[94] P. 85, Arnold, "The True Costs of Financial Sanctions."
[95] Caytas, "Weaponizing Finance."
[96] Sam Fleming, Philip Stafford and Jim Brunsden, "US and EU Head for Showdown over Shutting Iran off from Finance," *Financial Times*, May 17 (2018); Richard Goldberg and Mark Dubowitz, "To Help Iran, Angela Merkel Tries to Pull a Fast one with SWIFT," *Wall Street Journal*, June 20 (2018).

US sanctions by delisting key Iranian institutions, while publicly maintaining that it was doing so to maintain the stability of the overall financial system. US pressure has led European politicians such as German Foreign Minister Heiko Maas to begin discussing whether the EU needs to start building its own international financial payment channels, providing it with an alternative hub that is less vulnerable to US pressure.[97] It is unclear, however, whether the EU is capable of building the necessary institutions to challenge the U.S., given both internal political battles and external U.S. pressure against individual E.U. member states.[98]

The weaponization of SWIFT runs counter to the expectations of liberal accounts of globalization. It demonstrates how globalized networks can indeed be used to exercise "power over," both by gathering enormous amounts of data that can then be employed for security purposes, and by systematically excluding states from participation in the world financial system. Exactly because the SWIFT organization was a crucial hub in global economic exchange, it allowed those states that had jurisdictional sway over it to employ the panopticon and chokepoint effects, just as our framework expects. Furthermore, the topology and existence of the global financial network provided the U.S. (and the E.U.) with extraordinary strategic resources. Without this network structure, both powers would not have been able to access data e.g. on strategically important financial flows between third countries. In a counterfactual world, where the U.S. and the E.U. could only have unilaterally denied access to their own markets, or invoked bilateral dependencies to squeeze their adversaries, their efforts would have been far less effective, because adversary states could readily have turned to other financial partners.

---

[97] Heiko Maas, "Wir Lassen Nicht zu, Dass die USA uber Unsere Kopfe Hinweg Handeln," *Handelsblatt,* August 28, 2018. Available at https://www.handelsblatt.com/meinung/gastbeitraege/gastkommentar-wir-lassen-nicht-zu-dass-die-usa-ueber-unsere-koepfe-hinweg-handeln/22933006.html.

[98] Adam Tooze and Christian Odendahl, *Can the Euro Rival the Dollar* (London: Center for European Reform 2018).

The National Security Agency, PRISM and Counter-terrorism

The U.S. enjoyed similar – and arguably even greater – dominance over information networks and e-commerce firms, thanks to asymmetric network structures. It was far less eager to deploy the chokepoint effect, however. This reflected strategic calculation of benefits – the U.S. believed that a general diffusion of communication technology and the global dominance of U.S. e-commerce firms was in its interests. It also reflected domestic institutional constraints. The U.S. had effectively pre-committed to keeping e-commerce free from government control, except for truly compelling problems such as child pornography. This commitment meant that it had relatively few tools to oblige technology companies to do its bidding, and even where it did have such means, its commitment to openness imposed difficult trade-offs. Thus, for example, the U.S. sanctions regime applied to technology companies as well as other commercial actors, but the US created specific (if dubiously beneficial) carve-outs (specific exceptions to the sanctions) intended to allow technology companies to support openness in Iran and other regimes subject to U.S .sanctions.[99]

The U.S., under the Bill Clinton, George W. Bush and Barack Obama administrations, saw the spread of Internet openness as linked to the spread of democracy, and thus strategically beneficial for the U.S., as well as reflecting U.S. values.[100] In a much remarked upon speech,

[99] See Daniel Kehl, "US Government Clarifies Tech Authorizations under Iranian Sanctions," *New America*, February 14, 2014.
[100] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York, NY: Basic Books); Daniel McCarthy, "Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet," *Foreign Policy Analysis* Vol. 7, No. 1 (2011) pp.89-111; Ryan David Kiggins, "Open for Expansion: US Policy and the

Secretary of State Clinton depicted the Internet as a "network that magnifies the power and potential of all others," warning of the risks of censorship and celebrating the "freedom to connect" to "the internet, to websites, or to each other."[101] If the U.S. was to convince other states to refrain from controlling the Internet, it also had to restrain itself, and moreover needed to ensure that the Internet was not seen by other countries as a tool of direct U.S. influence. Thus, the U.S. largely refrained from overt pressure on e-commerce firms to help it achieve specific political outcomes. In one exceptional instance, a U.S. official asked Twitter officials to delay a temporary technical shutdown in the middle of the 2009 protests in Iran, on the belief that Twitter was playing an important part in helping organize the protests.[102] The action was controversial, and was not publicly repeated. The U.S. also saw substantial commercial advantage in an open Internet, warning that if states lapsed into "digital protectionism" then "global scalability – and thus the fate of American digital entrepreneurialism – will falter."[103]

Finally, the U.S. government sought to protect ICANN from a series of rearguard actions in the United Nations and other forums. When it appeared in 2005 that the EU might align itself with non-democratic countries to move authority over domain names to a more conventional

---

Purpose for the Internet in the Post-Cold War Era," *International Studies Perspectives*, Vol. 16, No. 1 (2015), pp.86-105.

[101] Hillary Clinton, *Remarks on Internet Freedom*, speech given at the Newseum, Washington DC, January 21, 2010. Available at https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[102] Mark Landler and Brian Stelter, "Washington Taps into a Potent New Force," *The New York Times,* June 16, 2009. http://www.nytimes.com/2009/06/17/world/middleeast/17media.html?_r=1&scp=2&sq=Twitter&st=cse.

[103] Remarks by Deputy US Trade Representative Robert Holleyman to the Commonwealth Club of San Francisco, March 30, 2016. Available at https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2016/march/Remarks-Deputy-USTR-Holleyman-Commonwealth-Club-TPP-Digital-Economy.

international organization, the U.S. pushed back forcefully.[104] Renewed pressure in 2012 combined with the Snowden revelations (the release of documents by Edward Snowden, a former NSA contractor, in 2013) to put the U.S. in a more awkward position – it finally accepted that ICANN needed to be separated from the U.S. government, and did so in the closing days of the Obama administration.[105]

Even while the U.S. declined to use chokepoints and promoted the cause of an open Internet, it took enormous advantage of the panopticon effect. The concentration of network hubs and e-commerce firms within the U.S. offered extraordinary benefits for information gathering, which the US was swift to take advantage of, especially after the September 11 attacks. After the attacks, the U.S. government quickly moved to leverage this advantage through the STELLARWIND program, which caused internal consternation within the Bush administration, and was eventually found by the Office of Legal Counsel to be illegal. It was soon replaced, however, by a variety of other programs designed to take advantage of the United States' unparalleled location at the heart of global networks of information exchange. In the blunt description of a former director of the National Security Agency (NSA), Michael Hayden: "This is a home game for us. Are we not going to take advantage that so much of it goes through Redmond, Washington? Why would we not turn the most powerful telecommunications and computing management structure on the planet to our use?"[106] Redmond, Washington is the

---

[104] Segal, *The Hacked World Order.*
[105] Edward Moyer, "US Hands Internet Control to ICANN," *CNET*, October 1, 2016. https://www.cnet.com/news/us-internet-control-ted-cruz-free-speech-russia-china-internet-corporation-assigned-names-numbers/. Ted Cruz and other Republicans claimed that the US was giving away the Internet, and unsuccessfully sought a court injunction against this action.
[106] Quoted in Michael Hirsch, "How America's Top Companies Created the Surveillance State," *National Journal* July 26, 2013. Available at http://www.nextgov.com/cio-briefing/2013/07/analysis-how-americas-top-tech-companies-created-surveillance-state/67490/.

home city of Microsoft, but Hayden was likely referring more generally to the U.S. technology sector.

In some cases, the U.S. government was able to conduct surveillance through undisclosed direct relations with technology companies. Michael Hirsch describes how technology companies were simultaneously worried about being seen as "instruments of government" and willing to recognize that they needed to cooperate with the government on key issues.[107] Under the PRISM program, the U.S. government had substantial legal authority to compel the production of records and information regarding non-US individuals from technology companies.

In addition, the U.S. government demanded the cooperation of telecommunications companies in carrying out "upstream collection" of large amounts of data from U.S. companies such as AT&T that help run the Internet backbone. In the description of Ryan Gallagher and Marcy Wheeler, "According to the NSA's documents, it values AT&T not only because it 'has access to information that transits the nation,' but also because it maintains unique relationships with other phone and internet providers. The NSA exploits these relationships for surveillance purposes, commandeering AT&T's massive infrastructure and using it as a platform to covertly tap into communications processed by other companies." [108]

The U.S. can copy data in bulk and mine it later for valuable information, while superficially complying with US laws that distinguish between the data of U.S. and non-U.S.

---

[107] Hirsch, "America's Top Companies."
[108] Ryan Gallagher and Henrik Moltke "The NSA's Hidden Hubs in Eight US Cities," *The Intercept* (June 25, 2018), https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/ . See also, Marcy Wheeler, "Verizon Gets Out of the Upstream Surveillance Business," *Emptywheel.com*, May 6, 2017.

citizens ("incidental collection" of data on U.S. citizens is permissible).[109] It has gathered data from Internet exchange points, and from the cable landing stations where undersea cables reach dry land. This data provided it with an alternative source of information to PRISM, and also gave it direct reach into the internal data of US e-commerce firms without their knowledge and consent, tapping for example, into the communication flows through which Google reconciled data in different countries.

The Snowden revelations provoked political uproar, both in the US and elsewhere. The result was a series of legal reforms that partly limited US government access to the data of US citizens, as well as policy measures including a presidential policy directive intended to reassure allies that the US would not use their citizens' information in unduly invasive ways.

Other states certainly engaged in surveillance activities, including members of the European Union (European privacy law does not currently prevent external surveillance for espionage, including European countries spying on each other, although it does restrict the ability of states to retain data on their own citizens). However, they lacked the "home advantage" of network centrality that Hayden described, and were correspondingly less able to gather useful information, so that the United States' European allies relied heavily on US willingness to share surveillance data for their own security.[110]

Summary

---

[109] For comprehensive descriptions of the various US electronic surveillance programs, see Laura K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age* (New York: Oxford University Press, 2016), and Jennifer Stisa Granick, *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It* (New York: Cambridge University Press 2017). Many of the legal interpretations that allow US surveillance are still unknown, as are the details of key programs.

[110] Spiegel Staff, "Der Unheimliche Dienst," *Der Spiegel*, May 2, 2015. http://www.spiegel.de/spiegel/print/d-134762481.html.

The internet has regularly been depicted, both in the scholarly literature and in US political debate, as a fundamentally liberal space characterized by open exchange and cooperation. This rhetoric serves to conceal the power dynamics that shape the relationship between the U.S. and online communications networks. For sure, the U.S. has not directly leveraged its dominance to create chokepoints, both because it lacks the domestic institutional capacity, and because several administrations have believed that its strategic and business interests are better served by open networks than the overt use of *force majeure*.[111] Yet the U.S. has also systematically exploited the panopticon effect to great benefit, and has been able to do so even when its allies have formally objected. This degree of information gathering power would be unthinkable either in a world where network forces did not tend to lead to grossly asymmetric outcomes benefiting states such as the U.S., or where states were limited to employing the tools of national markets and bilateral pressure.

Conclusions

There is a common trope in the literature on globalization, which suggests that greater economic exchange has fragmented and decentralized power relations. We, in contrast, argue that these economic interactions generate new structural conditions of power. Complex interdependence, like many other complex systems, may generate enduring power asymmetries.

This observation allows us to bring the literature on security, which has paid deep and sustained attention to the systemic and structural aspects of power, into direct debate with the

[111] McCarthy, "Open Networks," Kiggins, "Open for Expansion."

literature on global markets, which has largely neglected it. Theoretically, our account shows how the topography of networks shapes power relations, generating systematic differences in the ability of some states - and not others – to gather information and deny access to adversaries. Empirically, we show how decentralized patterns of economic exchange have led to centralized global networks such as SWIFT and the Internet. As we discuss further in unpublished research, similar patterns prevail in other global networks such as the dollar clearing system and some globalized supply chains. Bringing these findings together, our article provides a historically detailed account (1) of how the new network structures that shape power and statecraft have come into being, (2) how these structures have been used to weaponize interdependence by privileged actors (who possess both leverage over network hubs and the appropriate domestic institutions that allow them to exercise this leverage).

Our study has far-reaching implications for the study of international affairs. Our argument brings scholars of economic interdependence and security studies into closer dialogue with one another, generating important new insights for both. On the one hand, we press scholars of international political economy to grapple with the fact that institutions, which may serve to drive efficiency gains and reduce transaction costs, may also serve as sites of control. On the other hand, we push scholars of international security to consider how economic globalization creates its own set of international structures – global networks - and thus generates new forms of state power.[112]

[112] By examining such structures, scholars could speak better to other scholarship examining the role of networks in international security. See Goddard, "Embedded Revisionism," Alexander Coloey and Daniel Nexon, "The Empire Will Compensate You: The Structural Dynamics of the U.S. Overseas Basing Network," *Perspectives on Politics* Vol. 11, No. 4 (2013), pp. 1034-1050, Daniel Nexon and Thomas Wright, "What's at Stake in the American Empire Debate," *American Political Science Review* Vol. 101, No.3 (2007), pp. 253-271, Yonatan Lupu and Brian Greenhill,

Our findings further suggest that international relations scholars need to pay far more attention to the practical workings of networks than they do at present. There are thriving literatures on both international finance and cybersecurity. Both literatures largely discount the specific workings of the networks on which financial flows and cybersecurity depends. This is a serious mistake.

Our evidence from the cases of financial and digital communication furthermore offer important support for our theoretical claims. States need both leverage over network hubs and appropriate institutions if they are to take advantage of the panopticon and chokepoint effects. States and jurisdictions that have potential leverage over network hubs, but do not have the appropriate institutions, cannot make good use of weaponized interdependence. Thus, the European Union has fragmented instruments of financial regulation, which means that it has not been able to exercise control over SWIFT, except when its member states have agreed unanimously on formal sanctions under prodding from the U.S. Lacking a regulator like the Treasury Department's Office of Foreign Assets Control, or legal instruments like those that the U.S. introduced after September 11, 2001, it has not been able to deploy market control to influence non-E.U. banks, in the same ways that the US has. However, while we do not discuss it here, other research indicates that the E.U. is perfectly capable of leveraging market access in domains where it has both influence over key hubs and well-developed institutions (e.g., in the area of privacy).[113]

U.S. capacity to weaponize interdependence similarly depends on domestic institutions as well as the topology of global networks. Thus, for example, the existing institutional capacity of

---

"The Networked Peace: Intergovernmental Organizations and International Conflict," *Journal of Peace Research* Vol. 54, No. 6 (2017), pp.833-848.

[113] Henry Farrell and Abraham Newman, *Of Privacy and Power*; Nikhil Kalyanpur and Abraham Newman, "Mobilizing Market Power".

the NSA and new laws introduced after the September 11 attacks, allowed the US to deploy the panopticon effect to enormous advantage, gathering vast quantities of strategic information. However, it lacked the appropriate institutions to oblige US e-commerce companies to actively regulate other businesses and individuals or cut them out of the network, in the same way as it could use the US correspondent banking system to regulate global networks.

Our framework also suggests that there are broader limits to weaponized interdependence. Most importantly, not all markets rest directly on asymmetric networks. For example, international oil markets are sufficiently diversified that they are relatively liquid, and thus present no single point of control.[114] Where there are no network asymmetries, it will be difficult to weaponize interdependence. Moreover, not all sectors have been internationalized or rest heavily on networks of exchange. Finally, states that are less well integrated into the international economy are correspondingly less likely to be vulnerable to information gathering, while their vulnerability to the threatened or actual use of chokepoints will depend on the degree of autarky they have achieved.

We have now entered into a new stage of network politics, in which other states have begun to respond to such efforts. When interdependence is used by privileged states for strategic ends, other states are likely to start considering economic networks in strategic terms too. Targeted states – or states that fear they will be targeted – may attempt to isolate themselves from networks, look to turn network effects back on their more powerful adversaries, and even, under some circumstances, reshape networks so as to minimize their vulnerabilities or increase

[114] Long and Hughes, "Is There an Oil Weapon." There may be more complex strategic questions and knock-on consequences: see Caitlin Talmadge, "Closing Time: Assessing the Iranian Threat to the Strait of Hormuz," *International Security* Vol 33, No. 1 (Summer 2008), pp. 82-117.

the vulnerabilities of others.[115] Hence, the more that privileged states look to take advantage of their privilege, the more that other states and nonstate actors will take action that might potentially weaken or even undermine the interdependent features of the preexisting system.[116] The ability of states to resist weaponized interdependence will reflect, in part, their degree of autonomy from those economic interests that seek to maintain the benefits of centralized exchanges even in the face of greater constraints on state authority.

The U.S. and its allies find themselves in a new and uncertain world, where rival powers and adversaries are seeking to insulate themselves from global networks, and perhaps over the longer run to displace these networks. Our arguments do not provide precise predictions as to the strategies that rivals and adversaries will deploy, although they do suggest how these strategies will be shaped by rival states' own national institutions and network positions. They highlight the importance of enduring, but not immutable network structures. States are locked into existing network structures only up to that point where the costs of remaining in them are lower than the benefits, and should this change, we may see transitions to new arrangements.

Thus, for example, the initial US decision to exclude the Chinese firm ZTE from global supply chains appears to have precipitated a major reconsideration by the Chinese government of China's reliance on foreign chip manufacturers and of the need for China to create its own domestic manufacturing capacities to mitigate its economic vulnerabilities.[117] This policy

---

[115] Henry Farrell and Abraham Newman, "The Janus Face of the Liberal Information Order," paper presented at the IO@75 Workshop, 2018, Henry Farrell and Bruce Schneier, *Common Knowledge Attacks on Democracy*, Berkman-Klein Center for Internet and Society at Harvard University research paper, October 2018.

[116] Commercial actors too may look to disentangle themselves when the costs of state control start to exceed the benefits of network economies.

[117] Jones, "Unintended Consequences," Edward White, "China Seeks Semiconductor Security in Wake of ZTE Ban," *Financial Times* June 18, 2018. https://www.ft.com/content/a1a5f0fa-63f7-11e8-90c2-9563a0613e56.

reoirinetation surely involves efforts to mitigate bilateral asymmetric vulnerabilities of the kind emphasized in traditional liberal accounts. However, it may also require the reconfiguration of entire networks of interlocking supply chains with global consequences. Similar concerns led to initial US suspicion of Huawei and ZTE, and fears that their telecommunications equipment may have built-in vulnerabilities to assist Chinese surveillance. As interdependence becomes increasingly weaponized, global supply chains may unravel.

Western threats to weaponize SWIFT against Russia in the wake of the Ukraine crisis produced similar responses.[118] Then Prime Minister Dimitry Medvedev threatened that "our economic reaction and generally any other reaction will be without limits," while the chief executive of VTB, a major Russian bank, said it would mean that "the countries are on the verge of war, or they are definitely in a cold war."[119] In a major foreign policy speech, President Vladimir Putin warned that "politically motivated sanctions have only strengthened the trend towards seeking to bolster economic and financial sovereignty and countries' or their regional groups' desire to find ways of protecting themselves from the risks of outside pressure. We already see that more and more countries are looking for ways to become less dependent on the dollar and are setting up alternative financial and payments systems and reserve

[118] Gideon Rachman, "The Swift way to Get Putin to Scale Back His Ambitions," *Financial Times*, May 12, 2014. https://www.ft.com/content/d6ded902-d9be-11e3-920f-00144feabdc0; Economist staff writers, "Too smart by Half?: Effective Sanctions Have Always Been Hard to Craft," *The Economist*, September 6, 2014. https://www.economist.com/briefing/2014/09/06/too-smart-by-half; Economist staff writers, "The Pros and Cons of a SWIFT Response," *The Economist*, November 20, 2014. https://www.economist.com/international/2014/11/20/the-pros-and-cons-of-a-swift-response.

[119] TASS staff writers, "Russia to Respond to Possible Disconnection from SWIFT," *TASS*, January 27, 2015. http://tass.com/russia/773628; Gillian Tett and Jack Farchy, "Russian Banker Warns West over Swift," *Financial Times*, January 23, 2015.

currencies. I think that our American friends are quite simply cutting the branch they are sitting on."[120]

This may help explain Russia's apparent reported interest in creating a blockchain based payment system for the Eurasian Economic Union and other states interested in signing up.[121] Blockchain systems are designed to use "proof of work" or "proof of stake" and provable guarantees (systems based on mathematically secure theorems) to avoid any need for central authority (and hence any possibility of that authority being leveraged for political or other purposes).[122] In this way, a blockchain ledger for financial transactions could mute chokepoint strategies. That said, blockchain systems impose their own, sometimes quite unattractive risks and restrictions for state authorities.

Piecemeal worries over adversaries and resulting actions may erode global networks over the long term. More rapid change may occur if U.S. actions lead allies to seriously reconsider their exposure to global networks that they rely on far more heavily than China and Russia, but have not to this point seen as a threat vector. As Daniel Drezner has argued, the most plausible path to such a transition would involve the defection of U.S. allies, if they decided that the U.S. was abusing weaponized interdependence in ways that conflicted with their core interests.[123] Our account helps explain why this is so: it is the United States' West European allies that are most

---

[120] Vladimir Putin, *Welcoming Speech to Meeting of the Valdai International Discussion Club*, October 24, 2014. http://en.kremlin.ru/events/president/news/46860.
[121] Tass Staff Writer, "Bank of Russia Suggests FinTech's Ethereum Blockchain as Single System for EAEU," *TASS*, April 03, 2018. http://tass.com/economy/997474.
[122] For a tolerably accessible overview of the underlying technical issues, see Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton, NJ: Princeton University Press 2016). Popular accounts tend to underestimate the vulnerabilities of blockchain technologies.
[123] Daniel Drezner, "Could Walking Away From the Iran Deal Threaten the Dollar?"

likely to have control or potential control over key nodes in global networks, or to be credibly able to set up their own alternatives.

European states have been willing to accept US extraterritorial pressure, because of "shared democratic values and indeed economic interests."[124] Currently, they benefit more than they suffer from the US exercise of network hegemony. However, this acquiescence "implies that [the equilibrium of transatlantic relations] should not be disturbed by the abuse of that which certain people perceive as a form of imperium in the domain of law."[125] Policy-makers in Europe have started to explore financing options that are isolated from the US financial system. While the practical effect of these specific initiatives may be limited in the short term, they put in motion a potential decoupling. This sanitization process may possibly fall victim to infighting within and among allies, but might also generate its own internal self-reinforcing dynamics.[126] If the current war of words between Europe and the U.S. over secondary sanctions devolves into clashing standards and competing financial instruments, the U.S. may find that even its allies are no longer willing to use the networks that it has weaponized to project its power.

---

[124] Our translation, Karen Berger (Rapporteur), *Rapport d'Information Déposé en application de l'article 145 du Règlement par la Commission des Affaires Étrangeres et la Commission des Finances, en Conclusion des Travaux d'une Mission d'Information Constituée le 3 février 2016 sur l'Extraterritorialité de la Législation Américaine* (Paris, France: French General Assembly (Parliament) 2016). Available at http://www.assemblee-nationale.fr/14/rap-info/i4082.asp.
[125] Ibid.
[126] Robin Emmott, "EU Considers Iran Central Bank Transfers to Beat US sanctions," *Reuters*, May 18 (2018).