Weaponized Interdependence

How Global Economic Networks Shape State Coercion

Henry Farrell and Abraham L. Newman

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 United States. 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, tartly noted that the United States was not the "economic policeman of the planet."[2]

The reimposition of sanctions on Iran is just one recent example of how the United States 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

Henry Farrell is Professor of Political Science and International Affairs at George Washington University. Abraham L. Newman is Professor at the Edmund A. Walsh School of Foreign Service and the Government Department at Georgetown University.

The authors are grateful to Miles Evers, Llewellyn Hughes, Woojeong Jang, Erik Jones, Miles Kahler, Nikhil Kalyanpur, Matthias Matthijs, Kathleen McNamara, Daniel Nexon, Gideon Rose, Mark Schwartz, and William Winecoff, as well as the anonymous 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 2018 annual convention of the International Studies Association and at the Johns Hopkins University School of Advanced International Studies Research Seminar in Politics and Political Economy on April 17, 2018. The authors are also grateful to the participants and audiences at both events for feedback.

1. The legal principles through which exposure is determined are complex. For a useful 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, doi.org/10.2469/cp.v29.n3.2.
2. Anne-Sylvaine Chassany, Michael Peel, and Tobias Buck, "EU to Seek Exemptions from New U.S. Sanctions on Iran," *Financial Times*, May 9, 2018.
3. Henry Foy, "EN+ President Steps Down in Move to Win U.S. Sanctions Waiver," *Financial Times*, June 4, 2018.
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 2014/15), pp. 152–189, doi.org/10.1162/ISEC_a_00188; Jeff D. Colgan, "Fueling the Fire: Pathways from Oil to War," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 147–180, doi.org/10.1162/ISEC_a_00135; Charles L. Glaser, "How Oil Influences U.S. National Security: Reframing Energy Security," *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 112–146, doi.org/10.1162/ISEC_a_00137; and Llewelyn Hughes and Phillip Y. Lipscy, "The Politics of Energy," *Annual Review of Political Science*, Vol. 16, No. 1 (May 2013), pp. 449–469, doi.org/10.1146/annurev-polisci-072211-143240.

International Security, Vol. 44, No. 1 (Summer 2019), pp. 42–79, https://doi.org/10.1162/ISEC_a_00351

are rapidly coming to play similarly important roles. In Rosa Brooks's 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 that involve states denying outside access to their own markets individually or as an alliance).[8] Power and vulnerability are characterized as the consequences of aggregate market size or bilateral interdependencies. In addition, accounts that examine more dif-

5. Rosa Brooks, *How Everything Became War and the Military Became Everything: Tales from the Pentagon* (New York: Simon & 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, Conn.: Yale University Press, 2017).
7. Joanne Gowa, "Bipolarity, Multipolarity, and Free Trade," *American Political Science Review*, Vol. 83, No. 4 (December 1989), pp. 1245–1256, doi.org/10.2307/1961667; Brian M. Pollins, "Does Trade Still Follow the Flag?" *American Political Science Review*, Vol. 83, No. 2 (June 1989), pp. 465–480, doi.org/10.2307/1962400; John R. Oneal et al., "The Liberal Peace: Interdependence, Democracy, and International Conflict, 1950–85," *Journal of Peace Research*, Vol. 33, No. 1 (February 1996), pp. 11–28, doi.org/10.1177/0022343396033001002; and Dale C. Copeland, *Economic Interdependence and War* (Princeton, N.J.: Princeton University Press, 2014).
8. Robert A. Pape, "Why Economic Sanctions Do Not Work," *International Security*, Vol. 22, No. 2 (Fall 1997), pp. 90–136, doi.org/10.2307/2539368; Kimberly Ann Elliott, "The Sanctions Glass: Half Full or Completely Empty?" *International Security*, Vol. 23, No. 1 (Summer 1998), pp. 50–65, doi.org/10.2307/2539262; 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 (Winter 2000), pp. 80–107, doi.org/10.1162/016228899560248; Jonathan Kirshner, "Economic Sanctions: The State of the Art," *Security Studies*, Vol. 11, No. 4 (Summer 2002), pp. 160–179, doi.org/10.1080/714005348; Fiona McGillivray and Allan C. Stam, "Political Institutions, Coercive Diplomacy, and the Duration of Economic Sanctions," *Journal of Conflict Resolution*, Vol. 48, No. 2 (April 2004), pp. 154–172, doi.org/10.1177/0022002703262858; and Daniel W. Drezner, "Outside the Box: Explaining Sanctions in Pursuit of Foreign Economic Goals," *International Interactions*, Vol. 26, No. 4 (2001), pp. 379–410, doi.org/10.1080/03050620108434972, which does consider secondary sanctions, as does the policy literature we discuss below.

fuse 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 intersects with domestic institutions and norms to shape coercive authority. Our account places networks such as financial communications, supply chains, and the internet, which have been largely neglected by international relations scholars, at the heart of a compelling new understanding of globalization and power.[10] Globalization has transformed the liberal order, by moving the action away from multilateral interstate negotiations and toward networks of private actors.[11] This transformation 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 atten-

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. 3 (Spring 2009), pp. 789–822; and Daniel W. Drezner, "Targeted Sanctions in a World of Global Finance," *International Interactions*, Vol. 41, No. 4 (2015), pp. 755–764, doi.org/10.1080/03050629.2015.1041297. Secondary sanctions coexist with other tools to control international financial flows. For a useful recent overview, see Miles Kahler et al., *Global Governance to Combat Illicit Financial Flows: Measurement, Evaluation, Innovation* (Washington, D.C.: Council on Foreign Relations, 2018).

10. Of course, there is a burgeoning scholarship on cybersecurity, which is relevant to the internet. See Sarah E. Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics," Cornell University and U.S. Naval War College, 2018; Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 44–71, doi.org/10.1162/ISEC_a_00266; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 72–109, doi.org/10.1162/ISEC_a_00267; Henry Farrell and Charles L. Glaser, "The Role of Effects, Saliencies, and Norms in U.S. Cyberwar Doctrine," *Journal of Cybersecurity*, Vol. 3, No. 1 (March 2017), pp. 7–17, doi.org/10.1093/cybsec/tyw015; and Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, No. 3 (Winter 2014/15), pp. 7–47, doi.org/10.1162/ISEC_a_00189. This literature, however, largely fails to address the network characteristics of the internet, focusing instead on variation in traditional metrics such as the offense-defense balance, the ability to deter or compel, and the treatment of 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 United States will have a different set of strengths and vulnerabilities than states that 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, Calif.: 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*, July 2000, pp. 378–382, doi.org/10.1038/35019019.

11. Kathryn Judge, "Intermediary Influence," *University of Chicago Law Review*, Vol. 82, No. 2 (Spring 2015), pp. 573–642, https://chicagounbound.uchicago.edu/uclrev/vol82/iss2/1.

tion 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 United States can exercise "power with" (the power to work together constructively with allies) to achieve liberal objectives.[12]

Our alternative account makes a starkly different assumption, providing a structural explanation 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 demonstrates 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

12. See Robert O. Keohane and Joseph S. Nye Jr., *Power and Interdependence*, 4th ed. (New York: 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 (Fall 2002), pp. 1–92; Anne-Marie Slaughter, "Global Government Networks, Global Information Agencies, and Disaggregated Democracy," *Michigan Journal of International Law*, Vol. 24, No. 4 (Summer 2003), pp. 1044–1075, https://repository.law.umich.edu/mjil/vol24/iss4/7; Anne-Marie Slaughter, *A New World Order* (Princeton, N.J.: Princeton University Press, 2004); and Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World* (New Haven, Conn.: 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 (April 1991), pp. 336–366, doi.org/10.2307/2010398.

13. Albert-László Barabási and Réka Albert, "Emergence of Scaling in Random Networks," *Science*, October 1999, pp. 509–512, doi.org/10.1126/science.286.5439.509; M.E.J. Newman and Juyong Park, "Why Social Networks Are Different from Other Types of Networks," *Physical Review E*, September 2003, pp. 1–8, doi.org/10.1103/PhysRevE.68.036122; Aaron Clauset, Cosma Rohilla Shalizi, and M.E.J. Newman, "Power-Law Distributions in Empirical Data," *SIAM Review*, Vol. 51, No. 4 (December 2009), pp. 661–703, doi.org/10.1137/070710111; Emilie M. Hafner-Burton, Miles Kahler, and Alexander H. Montgomery, "Network Analysis for International Relations," *International Organization*, Vol. 63, No. 3 (Summer 2009), pp. 559–592, doi.org/10.1017/S0020818309090195; and Stacie E. Goddard, "Embedded Revisionism: Networks, Institutions, and Challenges to World Order," *International Organization*, Vol. 72, No. 4 (Fall 2018), pp. 763–797, doi.org/10.1017/S0020818318000206.

which states can gain powerful advantages from weaponizing interdependence; they respectively rely on the panopticon and chokepoint effects of networks. In the former, advantaged states use their network position to extract informational advantages vis-à-vis adversaries, whereas in the latter, they can cut adversaries off from network flows.

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 nonproliferation, counterterrorism, and great power competition. Moreover, global finance and the internet are often depicted as being at the vanguard of decentralized economic networks. 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 communications see important variation in the level and kind of control that they offer to influential states. In the former, the United States, in combination with its allies, has sufficient jurisdictional grasp and appropriate domestic institutions to oblige hub actors to provide it with information and to cut off other actors and states. In internet communications, the United States 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 United States 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 United States will be able to exercise the panopticon effect even without the consent of its allies, but it 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 United States market size or military power. Empirically, the cases draw on extensive readings of the primary and secondary literature as well as interviews with key policymakers.

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

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, https://asia.nikkei.com/Economy/Trade-war/Huawei-freeze-chills-global-supply-chain.

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—including 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 states, 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 United States. We conclude by considering the policy implications of clashes between countries such as the United States 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 difficult 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 manufac-

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 (April 2011), pp. 311–341, doi.org/10.1017/S002081831100004X.

ture 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 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 has 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 United States 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 there are multiple different possible hubs, reducing the dominance of great powers such as the United States. 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 web

16. Robert O. Keohane, "The Old IPE and the New," *Review of International Political Economy*, Vol. 16, No. 1 (February 2009), pp. 34–46, at pp. 36–37, doi.org/10.1080/09692290802524059.
17. Keohane and Nye, *Power and Interdependence*, p. 253.
18. Ibid.
19. Nye, "Deterrence and Dissuasion in Cyberspace."
20. Raustiala, "The Architecture of International Cooperation"; Slaughter, *A New World Order*; and Slaughter, *The Chessboard and the Web*.

connecting a network of points 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 topologies in which exchange becomes centralized, flowing through a few specific intermediaries.[23] Contrary to Keohane and Nye's predictions, key global economic networks have converged toward "hub and spoke" systems, with important consequences for power relations.[24]

---

21. Slaughter, *The Chessboard and the Web*, p. 163.

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 (February 2016), pp. 4–18, doi.org/10.1093/jogss/ogv007; 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 (April 2017), pp. 203–231, doi.org/10.1080/09692290.2017.1308417; Seva Gunitsky, "Complexity and Theories of Change in International Politics," *International Theory*, Vol. 5, No. 1 (March 2013), pp. 35–63, doi.org/10.1017/S1752971913000110; and Thomas Oatley, "Toward a Political Economy of Complex Interdependence," *European Journal of International Relations*, forthcoming, doi.org/10.1177/1354066119846553.

23. John F. Padgett and Christopher K. Ansell, "Robust Action and the Rise of the Medici, 1400–1434," *American Journal of Sociology*, Vol. 98, No. 6 (May 1993), pp. 1259–1319, doi.org/10.1086/230190; and Judge, "Intermediary Influence."

24. Our argument builds on Susan Strange's notion of "structural power." See, for example, 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 Randall Germain, ed., *Susan Strange and the Future of Global Political Economy: Power, Control, and Transformation* (London: Routledge, 2016). For different accounts, see Philip G.

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 actors, which aggregate to produce structures that influence their behavior. Specifically, the market-focused strategies of 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)

Cerny, *Rethinking World Politics: A Theory of Transnational Neopluralism* (New York: Oxford University Press, 2010); and Louis W. Pauly, "The Anarchical Society and a Global Political Economy," in Hidemi Suganami, Madeline Carr, and Adam Humphreys, eds., *The Anarchical Society at 40: Contemporary Challenges and Prospects* (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).

25. Newman and Park, "Why Social Networks Are Different from Other Types of Networks." An important literature in statistical physics and related disciplines studies the topology of large-scale networks and how topology shapes, for example, processes of contagion. See Duncan J. Watts, "The 'New' Science of Networks," *Annual Review of Sociology*, Vol. 30, No. 1 (2004), pp. 243–270, doi.org/10.1146/annurev.soc.30.020404.104342; and, for a useful overview, Mark Newman, Albert-László Barabási, and Duncan J. Watts, eds., *The Structure and Dynamics of Networks* (Princeton, N.J.: Princeton University Press, 2011). This literature has been underused by political scientists. For recent exceptions, see Hafner-Burton, Kahler, and Montgomery, "Network Analysis for International Relations"; Goddard, "Embedded Revisionism"; Miles Kahler, ed., *Networked Politics: Agency, Power, and Governance* (Ithaca, N.Y.: Cornell University Press, 2009); Thomas Oatley, *A Political Economy of American Hegemony: Buildups, Booms, and Busts* (New York: Cambridge University Press, 2015); and Brandon J. Kinne, "Defense Cooperation Agreements and the Emergence of a Global Security Network," *International Organization*, Vol. 72, No. 4 (Fall 2018), pp. 799–837, doi.org/10.1017/S0020818318000218.

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 no need for network infrastructure are unlikely to be subject to the dynamics we discuss here. We return to this point in the conclusion.

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 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 do 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 to-

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 (February 2007), pp. 58–88, doi.org/10.1177/0022002706296157; and Aaron Clauset, "Trends and Fluctuations in the Severity of Interstate Wars," *Science Advances*, Vol. 4, No. 2 (February 2018), pp. 1–9, doi.org/10.1126/sciadv.aao3580.

28. See Herbert A. Simon, "On a Class of Skew Distribution Functions," *Biometrika*, Vol. 42, Nos. 3/4 (December 1955), pp. 425–440, doi.org/10.2307/2333389; and Barabási and Albert, "Emergence of Scaling in Random Networks."

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 (May 1999), pp. 397–420, doi.org/10.1002/(SICI)1097-0266(199905)20:5<397::AID-SMJ35>3.0.CO;2-K; and Stephen P. Borgatti and Rob Cross, "A Relational View of Information Seeking and Learning in Social Networks," *Management Science*, Vol. 49, No. 4 (April 2003), pp. 432–445, doi.org/10.1287/mnsc.49.4.432.14428.

30. W. Brian Arthur, "Competing Technologies, Increasing Returns, and Lock-In by Historical Events," *Economic Journal*, March 1989, pp. 116–131, doi.org/10.2307/2234208; and Paul A. David, "Clio and the Economics of QWERTY," *American Economic Review*, Vol. 75, No. 2 (May 1985), pp. 332–337, https://www.jstor.org/stable/1805621.

pologies 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.

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 United States and the United Kingdom 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 toward nodes in advanced industrial democracies such as the United States and (to a lesser extent) the United Kingdom.[34]

This activity is often driven by an economic logic. In a networked world, businesses frequently 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 nonprofit actors, there are strong 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.

---

31. Thomas Oatley et al., "The Political Economy of Global Finance: A Network Model," *Perspectives on Politics*, Vol. 11, No. 1 (March 2013), pp. 133–153, doi.org/10.1017/S1537592712003593; and Oatley, *A Political Economy of American Hegemony*.

32. Réka Albert, Hawoong Jeong, and Albert-László Barabási, "Diameter of the World-Wide Web," *Nature*, September 1999, pp. 130–131, doi.org/10.1038/43601; Stefania Vitali, James B. Glattfelder, and Stefano Battiston, "The Network of Global Corporate Control," *PloS One*, Vol. 6, No. 10 (October 2011), e25995, pp. 1–6, doi.org/10.1371/journal.pone.0025995; and Camelia Miniou and Javier A. Reyes, "A Network Analysis of Global Banking: 1978–2010," *Journal of Financial Stability*, Vol. 9, No. 2 (June 2013), pp. 168–184, doi.org/10.1016/j.jfs.2013.03.001.

33. On trade, see Giorgio Fagiolo, Javier Reyes, and Stefano Schiavo, "World-Trade Web: Topological Properties, Dynamics, and Evolution," *Physical Review E*, Vol. 79, No. 036115 (March 2009), pp. 1–19, doi.org/10.1103/PhysRevE.79.036115; and Luca De Benedictis and Lucia Tajoli, "The World Trade Network," *World Economy*, Vol. 34, No. 8 (August 2011), pp. 1417–1454, doi.org/10.1111/j.1467-9701.2011.01360.x. On finance, see Oatley et al., "The Political Economy of Global Finance"; and William Kindred Winecoff, "Structural Power and the Global Financial Crisis: A Network Analytical Approach," *Business and Politics*, Vol. 17, No. 3 (October 2015), pp. 495–525, doi.org/10.1515/bap-2014-0050.

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 (October 2002), pp. 13382–13386, doi.org/10.1073/pnas.172501399.

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 toward a different one.

For example, Facebook's business model is centered on monetizing individuals' social networks through targeted advertisement and other means. It has resisted 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 the Society for Worldwide Interbank Financial Telecommunication (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 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 United States 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 high degree, and most other nodes are dependent on them. Once these topologies become established, it is difficult for economic actors to change or substantially displace them.

---

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*, Vol. 27 (June 2018), pp. 960–979, https://www.yalelawjournal.org/forum/the-ideological-roots-of-americas-market-power-problem; and Lina M. Khan, "Amazon's Antitrust Paradox," *Yale Law Journal*, Vol. 126, No. 3 (January 2017), pp. 710–805, https://www.yalelawjournal.org/note/amazons-antitrust-paradox.

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

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 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 forms of weaponi-

37. George E. Shambaugh IV, "Dominance, Dependence, and Political Power: Tethering Technology in the 1980s and Today," *International Studies Quarterly*, Vol. 40, No. 4 (December 1996), pp. 559–588, doi.org/10.2307/2600891; Beth A. Simmons, "The International Politics of Harmonization: The Case of Capital Market Regulation," *International Organization*, Vol. 55, No. 3 (Summer 2001), pp. 589–620, doi.org/10.1162/00208180152507560; Daniel W. Drezner, *All Politics Is Global: Explaining International Regulatory Regimes* (Princeton, N.J.: Princeton University Press, 2007); and Nikhil Kalyanpur and Abraham L. Newman, "Mobilizing Market Power: Jurisdictional Expansion as Economic Statecraft," *International Organization*, Vol. 73, No. 1 (Winter 2019), pp. 1–34, doi.org/10.1017/S0020818318000334.

38. Keohane and Nye, *Power and Interdependence*; Gowa, "Bipolarity, Multipolarity, and Free Trade"; Pollins, "Does Trade Still Follow the Flag?"; Oneal et al., "The Liberal Peace"; and Copeland, *Economic Interdependence and War*.

zation. 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 well. 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 sources of information. New technologies such as cell phones become active sensors. Under the panopticon effect, states' direct surveillance abilities may be radically outstripped by their capacity to tap into the information-gathering and information-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. 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

39. Harold James, "Cosmos, Chaos: Finance, Power, and Conflict," *International Affairs*, Vol. 90, No. 1 (January 2014), pp. 37–57, at p. 43, doi.org/10.1111/1468-2346.12094.
40. Ibid., p. 54.

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 substantial consequences. Again, there is some historical precedent for this phenomenon. Nicholas Lambert describes how the United Kingdom 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 its adversaries, weaponizing the global trading system.[41] As Heidi Tworek argues, Germany responded to the UK 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 economic 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 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

41. Nicholas A. Lambert, *Planning Armageddon: British Economic Warfare and the First World War* (Cambridge, Mass.: Harvard University Press, 2012).
42. Heidi J.S. Tworek, *News from Germany: The Competition to Control World Communications, 1900–1945* (Cambridge, Mass.: Harvard University Press, 2019).
43. Sarah C. Kaczmarek and Abraham L. Newman, "The Long Arm of the Law: Extraterritoriality and the National Implementation of Foreign Bribery Legislation," *International Organization*, Vol. 65, No. 4 (Fall 2011), pp. 745–770, doi.org/10.1017/S0020818311000270; Kal Raustiala, *Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law* (New York: Oxford University Press, 2011); and Tonya L. Putnam, *Courts without Borders: Law, Politics, and U.S. Extraterritoriality* (New York: Cambridge University Press, 2016).

innovation in the most recent round of economic globalization. This geographic skew effectively means that only the United States and a couple of other key states and statelike entities (most notably, the European Union [EU] 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; alternatively, they may be able to prosecute strategies based only on panopticon effects and not on 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 constrain states from engaging in certain kinds of weaponization. Privacy laws in the EU, 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 European governments to directly exploit 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

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 (September 2007), pp. 827–846, doi.org/10.1080/13501760701497659; Elliot Posner, "Making Rules for Global Finance: Transatlantic Regulatory Cooperation at the Turn of the Millennium," *International Organization*, Vol. 63, No. 4 (October 2009), pp. 665–699, doi.org/10.1017/S0020818309990130; Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton, N.J.: Princeton University Press, 2011); and Kalyanpur and Newman, "Mobilizing Market Power."

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

46. Henry Farrell and Abraham L. Newman, "Making Global Markets: Historical Institutionalism in International Political Economy," *Review of International Political Economy*, Vol. 17, No. 4 (October 2010), pp. 609–638, doi.org/10.1080/09692291003723672; and Henry Farrell and Abraham L. Newman, "Domestic Institutions beyond the Nation-State: Charting the New Interdependence Approach," *World Politics*, Vol. 66, No. 2 (April 2014), pp. 331–363, doi.org/10.1017/S0043887114000057.

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 United States—were able to take advantage of these network structures, to exploit panopticon effects or chokepoint effects. Importantly, our cases offer variation in the ability of the United States 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 is reliable and secure communication between financial institutions regarding the multitude of transactions that occur globally on any given day.

Since the 1970s, interbank communication has been provided by SWIFT.[47] For much of the post–World 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 U.S. 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 U.S. 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 financial institutions involved. SWIFT's headquarters were established 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 data and beat competitors such as MARTI. In 1977, it was used in 22 countries by roughly

47. Our history of SWIFT draws from 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 (October/November 2014), pp. 21–30, doi.org/10.1080/00396338.2014.962797. For discussions of SWIFT in the EU-U.S. relationship, see Marieke de Goede, "The SWIFT Affair and the Global Politics of European Security," *Journal of Common Market Studies*, Vol. 50, No. 2 (March 2012), pp. 214–230, doi.org/10.1111/j.1468-5965.2011.02219.x; and 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 (March 2015), pp. 497–526, doi.org/10.1177/0010414014542330.

500 firms with annual traffic of approximately 3,000 messages. By 2016, it had become the dominant provider, serving more than 200 countries and some 11,000 financial institutions and carrying more than 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 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]

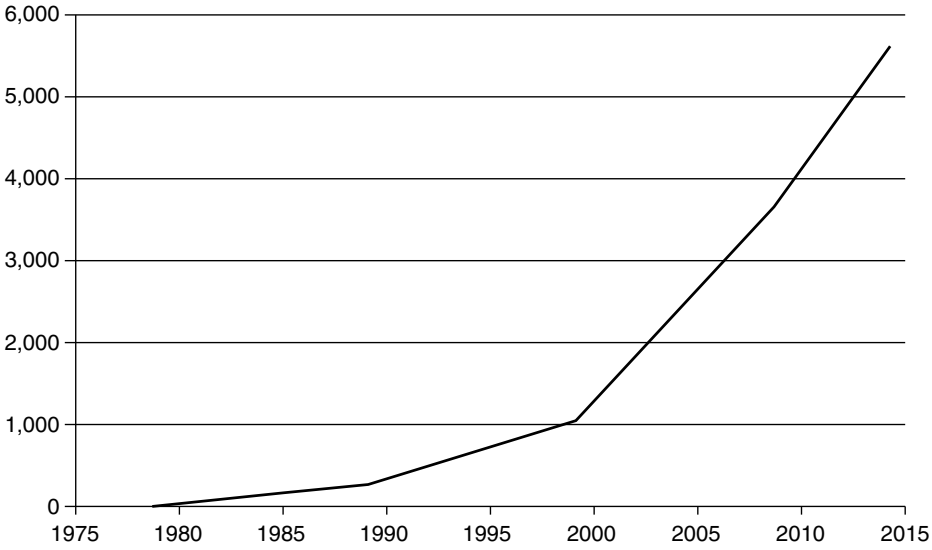
Eventually, the organization's dominance over financial messaging led to monopoly regulation by the Commission of the European Union. La Poste (the deregulated Postes, Télégraphes et Téléphones of France) sought access to the SWIFT network as part of its banking operations, and SWIFT denied the request on the grounds that La Poste was not a traditional banking institution. The European Commission's ruling in 1997 that SWIFT "holds a monopolistic position in the market for international payment message transfer" meant that it was a quasi utility and had to follow an open access model.[50] 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.[51] By the turn of the millennium, nearly all major global financial institutions used the SWIFT system to process their transactions (see figure 1).

The Internet—All Roads Lead through Northern Virginia

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 U.S. President Bill Clinton, believed that it was effectively invulnerable to control.[52] In contrast to

48. Scott and Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, p. 1.
49. Ibid., p. 107.
50. European Commission, "Following an Undertaking by S.W.I.F.T. to Change Its Membership Rules, the European Commission Suspends Its Action for Breach of Competition Rules," press release IP/97/870 (Brussels: European Commission, October 13, 1997), p. 2.
51. 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*, CEP Discussion Paper No. 992 (London: Center for Economic Performance, London School of Economics and Political Science, 2017), http://eprints.lse.ac.uk/id/eprint/83641.
52. William J. Clinton, remarks at the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, Washington, D.C., March 8, 2000.

Figure 1. Annual SWIFT Messages in Millions*



*SWIFT stands for Society for Worldwide Interbank Financial Telecommunication.

"centralized" networks such as the then-existing phone system, where different phones connected through a 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.[53] The Transmission Control Protocol/Internet Protocol allowed servers to speedily identify blockages in the system and find alternative routes for information. In such a system, government control seemed difficult; as the prominent activist John Gilmore put it, the "Net interprets censorship as damage, and routes around it."[54] This resistance to blockages led some online libertarians to forecast the withering of the state and a new age of human freedom.[55]

Contradicting these heady prognoses, the underlying architecture of the internet became increasingly centralized over time.[56] Some hubs and intercon-

53. On the theory of distributed networks, see Paul Baran, "On Distributed Communications Networks," *IEEE Transactions on Communications Systems*, Vol. 12, No. 1 (March 1964), pp. 1–9, doi.org/10.1109/TCOM.1964.1088883.
54. Philip Elmer-Dewitt, "First Nation in Cyberspace," *Time*, December 6, 1993, http://content.time.com/time/magazine/article/0,9171,979768,00.html.
55. John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Humanist*, Vol. 56, No. 3 (May/June 1996), p. 18.
56. Albert, Jeong, and Barabási, "Diameter of the World-Wide Web."

nections 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.[57] 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. Ninety-seven percent of intercontinental internet traffic travels across roughly 300 cables.[58] 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 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.[59]

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.[60] 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 small number of e-commerce companies. This dominance is in part thanks to U.S. government policy. The United States believed that, to the greatest extent possible, data governance should involve the free flow of content across borders (except, of course,

57. Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006); Ronald Deibert et al., eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, Mass.: MIT Press, 2008); Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2017); and Joshua A. Tucker et al., "From Liberation to Turmoil: Social Media and Democracy," *Journal of Democracy*, Vol. 28, No. 4 (October 2017), pp. 46–59, doi.org/10.1353/jod.2017.0064.

58. Asia-Pacific Economic Cooperation Secretariat, *Economic Impact of Submarine Cable Disruptions* (Singapore: APEC Policy Support Unit, February 2013).

59. Ibid.

60. See Patrick S. Ryan and Jason Gerson, "A Primer on Internet Exchange Points for Policymakers and Non-Engineers" (Rochester, N.Y.: Social Science Research Network, August 2012), doi.org/10.2139/ssrn.2128103; Kuai Xu et al., "On Properties of Internet Exchange Points and Their Impact on AS Topology and Relationship," in Nikolas Mitrou et al., eds., *Networking, 2004: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications* (Berlin: Springer-Verlag, 2004), pp. 284–295.

where this interfered with the intellectual property or other vital interests of U.S. corporations). It should furthermore be based primarily on self-regulation, looking to business cooperation and market structures to regulate their business relations with consumers.[61]

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 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.[62] The U.S. government scotched plans by Jon Postel, an early technological leader in internet communications, 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.[63]

Instead, it handed authority over domain names to a private nonprofit corporation under California law, the Internet Corporation for Assigned Names and Numbers (ICANN), which would work with for-profit entities to manage the technical aspects of coordination.[64] ICANN's ultimate authority stemmed from a contract with the Department of Commerce, which 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 U.S. 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 U.S. 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.[65] This section was intended for a specific 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

61. Henry Farrell interview with Ira Magaziner, New York City, New York, September 21, 2000.
62. White House, "A Framework for Global Electronic Commerce" (Washington, D.C.: White House, 1997).
63. Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge, Mass.: MIT Press 2009).
64. Ibid.
65. Jack M. Balkin, "The Future of Free Expression in a Digital Age," *Pepperdine Law Review*, Vol. 36 (2008), pp. 427–444.

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 firms. 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.[66] 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 the company with a nearly impregnable position, while Amazon's relentless growth into new marketplaces provided it with irresistible economies of scale.[67]

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.[68] As ever more online services move to cloud architectures, which store customer data and processing power in online data centers, cloud

66. See, more generally, Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, Mass.: Harvard University Press, 2015).
67. Khan, "Amazon's Antitrust Paradox."
68. See Laura DeNardis, "Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance," *Information, Communication & Society*, Vol. 15, No. 5 (June 2012), pp. 720–738, doi.org/10.1080/1369118X.2012.659199; and Tusikov, *Chokepoints*.

providers have emerged as central hubs.[69] 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).[70] 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 United States, and channel the most global data exchanges.

Weaponizing the Hubs

With the rise of these central hubs across financial messaging and online communication, states (in particular, the United States and members of the European Union) began to understand that they could exploit network properties to weaponize interdependence. In what follows, we use 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 United States 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 provides data about most global financial transactions and allows these transactions to take place. For the last twenty-five years, key states—most importantly, the United States—have gradually transformed the repository into a surveillance asset and financial sector dependence into a tool of asymmetric interdependence.

Although the terrorist attacks of September 11, 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 gover-

69. Bruce Schneier, "Censorship in the Age of Large Cloud Providers," *Lawfare* blog, June 7, 2018, https://lawfareblog.com/censorship-age-large-cloud-providers.
70. Benjamin Freed, "70 Percent of the World's Web Traffic Flows through Loudoun County," *Washingtonian*, September 14, 2016, https://www.washingtonian.com/2016/09/14/70-percent-worlds-web-traffic-flows-loudoun-county.

nance body focused on anti-money laundering, approached SWIFT in 1992.[71] FATF hoped to gain access to SWIFT records so as to track down illicit activity. At this 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."[72] 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 SWIFT 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.[73] 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 U.S. fight against terrorism, with the Treasury using the SWIFT system to monitor and investigate illicit activity.[74] As Juan Zarate, a former Treasury Department official, explained: "Access to SWIFT data would give the U.S. 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."[75]

71. 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 International Political Economy?" *International Politics*, Vol. 47, No. 6 (November 2010), pp. 617–637, doi.org/10.1057/ip.2010.32; and Anne L. Clunan, "The Fight against Terrorist Financing," *Political Science Quarterly*, Vol. 121, No. 4 (Winter 2006/07), pp. 569–596, doi.org/10.1002/j.1538-165X.2006.tb00582.x.

72. Scott and Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, p. 128.

73. For an excellent overview of both SWIFT and the dollar clearing system, see Joanna Diane Caytas, "Weaponizing Finance: U.S. and European Options, Tools, and Policies," *Columbia Journal of International Law*, Vol. 23, No. 2 (Spring 2017), pp. 441–475.

74. Eric Lichtblau and James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror," *New York Times*, June 23, 2006, https://www.nytimes.com/2006/06/23/washington/23intel.html.

75. Juan C. Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (London: Hachette, 2013), p. 50.

The SWIFT data became the Rosetta stone for U.S. counterterrorism operations, as it shed light on the complex networks of terrorist financing.[76] The government used the data as a key forensic tool to identify terrorist operations, co-conspirators, and planning. This effort became so central to U.S. and European counterterrorism operations that when it was challenged by European actors worried about civil liberties, the U.S. 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.[77] As one EU foreign minister concluded, "They pulled out all the moral and political stops."[78] 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."[79] Despite initial public protests, the dominant coalition in EU politics quietly approved of the U.S. use of SWIFT to create a financial data panopticon, so long as the United States was prepared to share the proceeds.[80]

U.S. and EU 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."[81] Caytas furthermore argues 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."[82]

As an example of the power of chokepoints, U.S. and European policymakers used SWIFT to reinforce the sanctions regime against Iran. A group of prominent U.S. policymakers, 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 contrib-

76. Lichtblau and Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror."
77. For a detailed discussion, see Henry Farrell and Abraham L. Newman, *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security* (Princeton, N.J.: Princeton University Press, 2019).
78. Hans-Jürgen Schlamp, "EU to Allow U.S. 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.
79. 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 United States for the Purposes of the Terrorist Finance Tracking Program* (Brussels: European Commission, 2017), p. 7.
80. Farrell and Newman, "The New Politics of Interdependence."
81. Caytas, "Weaponizing Finance," p. 449.
82. Ibid., p. 451.

uting to its economic health.[83] As per SWIFT's 2010 annual report, some nineteen Iranian banks as well as another twenty-five institutions relied on the messaging system.[84] 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."[85]

This campaign had consequences in both the United States and Europe. On February 2, 2012, the U.S. Senate Banking Committee adopted language that would have allowed the U.S. government to sanction SWIFT if it continued to allow Iranian financial institutions to use the SWIFT system, pushing the administration to adopt a more proactive stance.[86] The EU followed up on this threat in March, motivated by U.S. 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.[87]

The combination of EU and U.S. sanctions required SWIFT to cut Iranian banks out of its system. In 2012, the EU's Council banned the provision of financial messaging services to Iran.[88] 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."[89]

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

83. United Against Nuclear Iran (UANI), "SWIFT Campaign" (Washington, D.C.: UANI, 2012), https://www.unitedagainstnucleariran.com/index.php/swift.
84. SWIFT, *Annual Review, 2010: Common Challenges, Unique Solutions* (Brussels: SWIFT, 2010).
85. Ambassador Mark D. Wallace, letter re: SWIFT and Iran to Yawar Shah (Washington, D.C.: UANI, January 30, 2012), https://www.unitedagainstnucleariran.com/sites/default/files/IBR%20Correspondence/UANI_Letter_to_SWIFT_013012.pdf; and Jay Solomon and Adam Entous, "Banking Hub Adds to Pressure on Iran," *Wall Street Journal*, February 4, 2012, https://www.wsj.com/articles/SB10001424052970203889904577201330206741436.
86. Jay Solomon, *The Iran Wars: Spy Games, Bank Battles, and the Secret Deals That Reshaped the Middle East* (New York: Random House, 2016).
87. "U.S. Presses EU to Close SWIFT Network to Iran," Agence France-Presse, February 16, 2012; and Samuel Rubenfeld, "SWIFT to Comply with EU Ban on Blacklisted Entities," *Corruption Currents* blog, *Wall Street Journal*, March 15, 2018, https://blogs.wsj.com/corruption-currents/2012/03/15/swift-to-comply-with-eu-ban-on-blacklisted-entities.
88. Aaron Arnold, "The True Costs of Financial Sanctions," *Survival*, Vol. 58, No. 3 (June/July 2016), pp. 77–100; and "Iran Cut Off from Global Financial System," Associated Press, March 15, 2012.
89. UANI, "UANI Issues Statement following SWIFT's Announcement to Discontinue Services to EU-Sanctioned Iranian Financial Institutions," press release (Washington, D.C.: UANI, March 15, 2012), https://www.unitedagainstnucleariran.com/press-releases/uani-issues-statement-following-swift%E2%80%99s-announcement-discontinue-services-eu-sanction.

payment system. As explained by an EU official at the time, "It is a very efficient measure . . . It can seriously cripple the banking sector in Iran."[90]

Unwinding the SWIFT measures became a key bargaining point in the negotiations over Iran's nuclear program.[91] 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."[92] Accordingly, 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. Had the United States not imposed pressure, it is unlikely that the European Union would have been able to act on its own; as Caytas notes, the EU's fragmented internal decision-making structures and lack of supple institutions undermines its ability to weaponize finance.[93] Equally, the United States might have had difficulties in acting unilaterally in the face of concerted EU opposition, given SWIFT's primary location in Europe.

In 2018, the politics of the SWIFT chokepoint became more complex. As the United States backed out of the Iran deal, it threatened to reimpose SWIFT restrictions on Iran, while the EU resisted the re-weaponization of SWIFT.[94] SWIFT responded to the threat of U.S. sanctions by delisting key Iranian institutions, while publicly maintaining that it was doing so to maintain the stability of the overall financial system. U.S. 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 U.S. pressure.[95] It is unclear whether the EU is capable of building the necessary institutions to

90. 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, https://www.nytimes.com/2012/03/16/world/middleeast/crucial-communication-network-expelling-iranian-banks.html.
91. Zarate, *Treasury's War*.
92. Arnold, "The True Costs of Financial Sanctions," p. 85.
93. Caytas, "Weaponizing Finance."
94. Sam Fleming, Philip Stafford, and Jim Brunsden, "U.S. and EU Head for Showdown over Shutting Iran Off from Finance," *Financial Times*, May 17, 2018; and Richard Goldberg and Mark Dubowitz, "To Help Iran, Angela Merkel Tries to Pull a Fast One with SWIFT," *Wall Street Journal*, June 20, 2018.
95. Heiko Maas, "Wir lassen nicht zu, dass die USA uber unsere kopfe hinweg handeln" (We will not be sidelined by the USA), *Handelsblatt*, August 28, 2018, https://www.handelsblatt.com/meinung/gastbeitraege/gastkommentar-wir-lassen-nicht-zu-dass-die-usa-ueber-unsere-koepfe-hinweg-handeln/22933006.html.

challenge the United States, given both internal political battles and external U.S. pressure against individual EU member states.[96]

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 United States (and the EU) 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 United States and the EU could have unilaterally denied access only 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.

The National Security Agency, PRISM, and Counterterrorism

The United States 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 a strategic calculation of benefits; the United States 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 United States had effectively precommitted 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 United States 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.[97]

96. Adam Tooze and Christian Odendahl, *Can the Euro Rival the Dollar*? (London: Center for European Reform, 2018).
97. See Danielle Kehl, "U.S. Government Clarifies Tech Authorizations under Iranian Sanctions,"

The United States, 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 strategically beneficial for the United States, as well as reflecting U.S. values.[98] In a much remarked upon speech, 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."[99] If the United States 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 United States largely refrained from putting 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, in the belief that Twitter was playing an important part in helping organize the protests.[100] The action was controversial and was not publicly repeated. The United States 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."[101]

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 international organization, the United States pushed back forcefully.[102] Renewed pressure in 2012 combined with the Snowden revelations (the release of documents by

---

Open Technology Institute blog, New America, February 12, 2014, https://www.newamerica.org/oti/blog/us-government-clarifies-tech-authorizations-under-iranian-sanctions.

98. Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2012); Daniel R. McCarthy, "Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet," *Foreign Policy Analysis*, Vol. 7, No. 1 (January 2011), pp. 89–111, doi.org/10.1111/j.1743-8594.2010.00124.x; and Ryan David Kiggins, "Open for Expansion: U.S. Policy and the Purpose for the Internet in the Post–Cold War Era," *International Studies Perspectives*, Vol. 16, No. 1 (February 2015), pp. 86–105, doi.org/10.1111/insp.12032.

99. Hillary Rodham Clinton, "Remarks on Internet Freedom," speech given at the Newseum, Washington, D.C., January 21, 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

100. Mark Landler and Brian Stelter, "Washington Taps into a Potent New Force in Diplomacy," *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.

101. Deputy U.S. Trade Representative Robert Holleyman, "The Trans-Pacific Partnership and the Digital Economy," remarks at the Commonwealth Club of San Francisco, March 30, 2016, https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2016/march/Remarks-Deputy-USTR-Holleyman-Commonwealth-Club-TPP-Digital-Economy.

102. Segal, *The Hacked World Order*.

Edward Snowden, a former National Security Agency [NSA] contractor, in 2013) to put the United States 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.[103]

Even while the United States 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 United States offered extraordinary benefits for information gathering, which the United States 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 NSA director, 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?"[104] Redmond, Washington is the 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 worried about being seen as "instruments of government" but were willing to recognize that they needed to cooperate with the government on key issues.[105] Under the PRISM program, the U.S. government had substantial legal authority to compel the production of records and information regarding non-U.S. 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

103. Edward Moyer, "U.S. 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 United States was giving away the internet.
104. Quoted in Michael Hirsch, "How America's Top Companies Created the Surveillance State," *National Journal*, July 25, 2013, https://www.nationaljournal.com/s/628088/how-americas-top-tech-companies-created-surveillance-state.
105. Ibid.

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."[106]

The United States can copy data in bulk and mine it later for valuable information, while superficially complying with U.S. laws that distinguish between the data of U.S. and non-U.S. citizens ("incidental collection" of data on U.S. citizens is permissible).[107] 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 gave it direct reach into the internal data of U.S. 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, in both the United States and elsewhere. The result was a series of legal reforms that partly limited U.S. government access to the data of U.S. citizens, as well as policy measures including a presidential policy directive intended to reassure allies that the United States would not use their citizens' information in unduly invasive ways.

Other states certainly engaged in surveillance activities, including members of the EU (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 U.S. willingness to share surveillance data for their own security.[108]

---

106. Ryan Gallagher and Henrik Moltke, "The Wiretap Rooms: The NSA's Hidden Hubs in Eight U.S. Cities," *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* blog, May 6, 2017, https://www.emptywheel.net/2017/05/06/verizon-gets-out-of-the-upstream-business.

107. For comprehensive descriptions of the various U.S. 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 U.S. surveillance are still unknown, as are the details of key programs.

108. Maik Baumgärtner et al., "Der unheimliche dienst" (The eerie agency), *Der Spiegel*, May 2, 2015, http://www .spiegel.de/spiegel/print/d-134762481.html.

SUMMARY
The internet has regularly been depicted, both in the scholarly literature and in U.S. 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 United States and online communications networks. For sure, the United States 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*.[109] Yet, the United States 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 countries such as the United States or where states were limited to employing the tools of national markets and bilateral pressure.

Conclusion

There is a common trope in the literature on globalization that 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 literature on global markets, which has largely neglected it.[110] 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 demonstrate 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 of (1) how the new network structures that shape power and statecraft have come into being and (2) how these structures

109. McCarthy, "Open Networks"; and Kiggins, "Open for Expansion."
110. For a prescient exception, see Thomas Wright, "Sifting through Interdependence," *Washington Quarterly*, Vol. 36, No. 4 (Fall 2013), pp. 7–23, doi.org/10.1080/0163660X.2013.861706.

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 research 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—through global networks—and thus generates new forms of state power.[111] More generally, 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.

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 EU 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 United States. Lacking a regulator such as the Treasury Department's Office of Foreign Assets Control, or legal instruments such as those that the United States introduced after September 11, 2001, it has not been able to deploy market control to influence non-EU banks in the same ways that the United States has. However, although we do not discuss it here, other research indicates that the EU is perfectly capable of leveraging such control in domains where it has both influence over key hubs and well-developed institutions (e.g., in the area of privacy).[112]

111. By examining such structures, scholars could speak better to other scholarship examining the role of networks in international security. See Goddard, "Embedded Revisionism"; Alexander Cooley and Daniel H. Nexon, "'The Empire Will Compensate You': The Structural Dynamics of the U.S. Overseas Basing Network," *Perspectives on Politics*, Vol. 11, No. 4 (December 2013), pp. 1034–1050, doi.org/10.1017/S1537592713002818; Daniel H. Nexon and Thomas Wright, "What's at Stake in the American Empire Debate," *American Political Science Review*, Vol. 101, No. 3 (May 2007), pp. 253–271, doi.org/10.1017/S0003055407070220; and Yonatan Lupu and Brian Greenhill, "The Networked Peace: Intergovernmental Organizations and International Conflict," *Journal of Peace Research*, Vol. 54, No. 6 (November 2017), pp. 833–848, doi.org/10.1177/0022343317711242.

112. Farrell and Newman, *Of Privacy and Power*; and Kalyanpur and Newman, "Mobilizing Market Power."

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

Our framework also suggests that there are broader limits to weaponized interdependence. 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.[113] 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.

The world has 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 the vulnerabilities of others.[114] 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.[115] The ability of states to resist weaponized interdependence will reflect, in part, their de-

113. Hughes and Long, "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, doi.org/10.1162/isec.2008.33.1.82.

114. Henry Farrell and Abraham Newman, "The Janus Face of the Liberal Information Order," paper presented at the IO@75 Conference, Madison, Wisconsin, September 7–8, 2018; and Henry Farrell and Bruce Schneier, "Common-Knowledge Attacks on Democracy" (Cambridge, Mass.: Berkman Klein Center for Internet and Society, Harvard University, October 2018), https://cyber.harvard.edu/story/2018-10/common-knowledge-attacks-democracy.

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

gree of autonomy from those economic interests that hope to maintain the benefits of centralized exchanges even in the face of greater constraints on state authority.

The United States 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: should this change, one may see transitions to new arrangements.

Thus, for example, the initial U.S. 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.[116] This policy reorientation 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 U.S. suspicion of Huawei and ZTE and to fears that their telecommunications equipment may have built-in vulnerabilities that 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.[117] 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."[118] In a major foreign policy speech,

116. Jones and Whitworth, "The Unintended Consequences of European Sanctions on Russia"; and Edward White, "China Seeks Semiconductor Security in Wake of ZTE Ban," *Financial Times*, June 18, 2018.

117. Gideon Rachman, "The Swift Way to Get Putin to Scale Back His Ambitions," *Financial Times*, May 12, 2014; "Too Smart by Half? Effective Sanctions Have Always Been Hard to Craft," *Economist*, September 6, 2014, https://www.economist.com/briefing/2014/09/06/too-smart-by-half; and "The Pros and Cons of a SWIFT Response," *Economist*, November 20, 2014, https://www.economist.com/international/2014/11/20/the-pros-and-cons-of-a-swift-response.

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

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 currencies. I think that our American friends are quite simply cutting the branch they are sitting on."[119]

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.[120] 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).[121] 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 United States was abusing weaponized interdependence in ways that conflicted with their core interests.[122] Our account helps explain why this is so: it is the United States' West European allies that are most 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 U.S. extraterritorial pressure because of their "shared democratic values and indeed economic interests."[123]

119. Vladimir Putin, speech to meeting of the Valdai International Discussion Club, October 24, 2014, http://en.kremlin.ru/events/president/news/46860.
120. "Bank of Russia Suggests FinTech's Ethereum Blockchain as Single System for EAEU," TASS, April 3, 2018, http://tass.com/economy/997474.
121. For a tolerably accessible overview of the underlying technical issues, see Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton, N.J.: Princeton University Press, 2016). Popular accounts tend to underestimate the vulnerabilities of blockchain technologies.
122. Daniel W. Drezner, "Could Walking Away from the Iran Deal Threaten the Dollar?" *Washington Post*, August 12, 2015, https://www.washingtonpost.com/posteverything/wp/2015/08/12/could-walking-away-from-the-iran-deal-threaten-the-dollar.
123. Authors' translation of Karen Berger (rapporteur), *Rapport d'Information Déposé en application*

Currently, they benefit more than they suffer from the U.S. 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."[124] Policymakers in Europe have started to explore financing options that are isolated from the U.S. 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.[125] If the war of words between Europe and the United States over secondary sanctions devolves into clashing standards and competing financial instruments, the United States may face the slow erosion of its ability to weaponize key economic networks, constraining its ability to project power globally.

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 (Information report deposted pursuant to Article 145 of the Rules by the Foreign Affairs Commission and the Finance Committee in concluding the work of the Information Commission set up on February 3, 2016) (Paris: French General Assembly, October 5, 2016), http://www.assemblee-nationale.fr/14/rap-info/i4082.asp.

124. Ibid.

125. Robin Emmott, "EU Considers Iran Central Bank Transfers to Beat U.S. Sanctions," Reuters, May 18, 2018.