Weaponized Interdependence

By

Henry Farrell and Abraham L. Newman

DRAFT

In May 2018, the US Administration announced that it was pulling out of the Joint Comprehensive Plan of Action agreement on Iran's nuclear program, reimposing sanctions. Most notably, many penalties do not apply to US firms, but to foreign firms that may have no presence in the US; they are consequential in large part because of US importance to the global financial network.[1] This unilateral action by the US led to protest among America's European allies: France's Finance Minister, Bruno Le Maire, for example, tartly noted that America was not the "economic policeman of the planet."[2] Allies are exploring ways to circumvent US pressure, including tariffs and the use of direct money transfers to Iran's central bank to avoid US strictures.[3] However, within the US, opponents of Iran such as the Foundation for Defense of Democracies are pressing the US to take stronger measures, such as forcing the international banking messaging network SWIFT to "disconnect Iranian banks," by threatening individual members of SWIFT's board with penalties for sanctions evasion.[4]

---

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

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

[3] Robin Emmott, "EU Considers Iran Central Bank Transfers to Beat U.S. Sanctions, *Reuters* (Toronto: *Reuters* May 18, 2018), https://www.reuters.com/article/us-iran-nuclear-europe/eu-considers-iran-central-bank-transfers-to-beat-u-s-sanctions-idUSKCN1IJ100.

[4] Jenna Lifhits, "U.S., European Powers Could Clash Over Reimposition of Iran Sanctions," *The Weekly Standard* (Washington DC: The Weekly Standard, May 10, 2018), https://www.weeklystandard.com/jenna-lifhits/u-s-european-powers-could-clash-over-reimposition-of-iran-sanctions. See also Elizabeth Rosenberg, quoted as saying "The US could not be more clear that they are going after SWIFT," in Sam Fleming, Philip Stafford and Jim Brunsden, "US and EU Head for Showdown Over Shutting Iran Off From Finance," *Financial Times* (London: Financial Times, May 17, 2018), https://www.ft.com/content/04b831fc-5913-11e8-bdb7-f6677d2e1ce8. Iran hawks have long seen SWIFT as a crucial nexus of control. See, for example, Mark Dubowitz, "Congressional Testimony: The Iran Nuclear Deal and Its Impact on Terrorism Financing," Hearing before the House Financial Services Committee Task Force to Investigate Terrorism Financing, July 22, 2015 and Richard Goldberg, "If the U.S. Reimposes

This is just one recent example of how the US is using global economic networks to achieve its strategic aims.[5] While security scholars have long recognized the crucial importance of energy markets in shaping security outcomes,[6] financial and information markets are swiftly coming to play similarly important roles. In Rosa Brooks' evocative description, globalization has created a world in which 'everything became war.'[7] Flows of finance, information and physical goods across borders both create 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 which are unwilling to engage in direct conflict, may still employ 'all measures short of war.'[8]

These networks have security consequences because they increase interdependence between states that were previously relatively autonomous. Yet existing theory provides few useful guideposts as to how states may leverage network structures as a coercive tool and under what circumstances. It has focused instead on bilateral trade relations between dyadic pairs and

---

Sanctions on Iran, Allies Will Follow," *Foreign Policy* (Washington DC: Foreign Policy, October 2, 2017).

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

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

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

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

the vulnerabilities generated by those interactions.[9] Similarly, work on economic sanctions has yet to fully grasp the consequences of economic networks and how they are being weaponized. It primarily looks to explain the success or failure of primary sanctions – that is, sanctions which involve states denying outside access to their own markets individually or as an alliance.[10] Power and vulnerability are characterized as the consequences of aggregate market size or bilateral interdependencies. Moreover, accounts that examine more diffuse or secondary sanctions have focused more on comparative effectiveness than on theory building.[11]

In this manuscript, we develop a different understanding of state power, which links the specific topography and structure of economic networks to coercive authority. Our account places networks such as SWIFT and the Internet, which have gone largely neglected by international relations scholars, at the heart of a compelling new understanding of globalization

---

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

[10] Robert A. Pape, "Why Economic Sanctions Do Not Work," *International Security* Vol. 22, No. 2 (1997), pp. 90-136; Kimberly Ann Elliott, "The Sanctions Glass: Half Full or Completely Empty?," *International Security,* Vol. 23, No. 1 (1998), pp. 50-65; Daniel W. Drezner. *The Sanctions Paradox: Economic Statecraft and International Relations* (New York: Cambridge University Press, 1999); David A. Baldwin, "The Sanctions Debate and the Logic of Choice," *International Security*, Vol. 24, No. 3 (2000), pp. 80-107; Jonathan Kirshner, "Review Essay: Economic Sanctions: The State of the Art," *Security Studies* Vol. 11, No. 4 (2002), pp. 160-179; Fiona McGillivray, and Allan C. Stam. "Political Institutions, Coercive Diplomacy, and the Duration of Economic Sanctions," *Journal of Conflict Resolution* Vol. 48, No. 2 (2004), pp. 154-172.

[11] See Peter D. Feaver and Eric B. Lorber, *Coercive Diplomacy and the New Financial Levers: Evaluating the Intended and Unintended Consequences of Financial Sanctions* (London: Legatum Institute 2010); Orde F. Kittrie, "New Sanctions for a New Century: Treasury's Innovative Use of Financial Sanctions," *University of Pennsylvania Journal of International Law*, Vol. 30, No. 1 (2008), pp.789-822; Daniel Drezner, "Targeted Sanctions in a World of Global Finance," *International Interactions*, Vol. 41 (2015), pp. 755-64.

and power.[12] Globalization has transformed the global liberal order, by moving the action away from multilateral talking shops, and towards networks of private actors.[13] This has had crucial consequences for where state power is located in international politics, and how it is exercised.

We contrast our argument with recent liberal approaches such as those provided by Kal Raustiala and Anne-Marie Slaughter, who have constructed an extensive account of networked activity in a global order.[14] However, their arguments systematically neglect power asymmetries, depicting an idealized world in which liberal states such as the US can exercise "power with,"

---

[12] Of course, there is a burgeoning scholarship on cybersecurity, which is relevant to the Internet. See, for a few recent examples, Sarah Kreps and Jacquelyn Schneider, *Escalation Firebreaks in the Cyber, Conventional and Nuclear Domains: Moving Beyond Effects-Based Logics* (unpublished paper); Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* (2017) Vol. 41, No.3, pp.44-71; Rebecca Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes and Assessment," *International Security* (2017), Vol. 41, No. 3, pp. 72-109; Henry Farrell and Charles Glaser, "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine," *Journal of Cybersecurity* (2017) Vol.3, No.1, pp.7-17; Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* (2015) Vol. 39, No. 3, pp.7-47. However, this literature largely fails to address the network characteristics of the Internet, instead focusing on variation in traditional metrics such as the offense-defense balance, and the ability to deter or compel, tending to treat the network characteristics of the Internet either as a constant, or a straightforward determinant of state-level vulnerability or strength (so that technologically advanced states such as the US will have a different set of strengths and vulnerabilities than states which rely less on technology). An earlier proto-literature on 'netwar' examines how leaderless networks are becoming more important in world politics, but is primarily descriptive in nature. See John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica: Rand Corporation 1996). There is a technical literature that attends to the aspects of networks, but it too tends not to discuss the topological aspects we focus on below. For an important exception, see Réka Albert, Hawoong Jeong, and Albert-László Barabási, "Error and Attack Tolerance of Complex Networks;" *Nature*, Vol. 406, No. 6794 (2000), pp. 378-382.

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

[14] See Kal Raustiala,"The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law," *Virginia Journal of International Law* Vol. 43, No.1 (2002), pp.1-92; Anne-Marie Slaughter, "Global Government Networks, Global Information Agencies, and Disaggregated Democracy," *Michigan Journal of International Law* (2002), Vol. 24, pp.1044-1075; Anne-Marie Slaughter, *A New World Order* (Princeton NJ: Princeton University Press 2004); Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World* (New Haven, CT: Yale University Press 2017).

cooperating with distributed networks of non-state actors to achieve liberal objectives, so that interdependence decentralizes and flattens the distribution of power.

Our account stresses the crucial importance of power asymmetries, and the structural consequences of the topography of network structures. Here we draw on sociological and computational research on large-scale networks, which demonstrate the tendency of complex systems to create asymmetric network structures, in which some nodes are 'hubs,' and are far more connected than others.[15]

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 activate 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 specific strategies through which states can gain powerful advantages from weaponizing interdependence, the panopticon and chokepoint effects. In the former, network position is used to extract an information advantage vis-à-vis adversaries, while in the latter advantaged states can cut adversaries off from network flows.

---

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

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

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

Our argument has significant implications for scholars interested in thinking about the future of conflict in a world of global economic and information networks. For those steeped in

the liberal tradition, we demonstrate that institutions designed to generate market efficiencies and reduce transaction costs can be deployed for coercive ends. Focal points of cooperation become sites of control. For those researchers interested in conflict studies and the role of power, we show the critical role that economic relations play in modern warfare. Rather than rehashing more conventional debates on trade and conflict, however, we underscore how relatively new forms of economic interaction – financial and information flows – play a key role in strategic opportunities, stressing how the topography of global networks allows coercion. Here, we use basic insights from network theory to rethink what structural power means and thereby create new links between the literatures on economic and security relations, showing how coercive economic power can stem from structural characteristics of the global economy. Finally, the paper illustrates the deep empirical connection between economic networks – financial messaging, dollar clearing, internet communication – and a series of pressing real world questions – counter terrorism, rogue states, great power competition. We conclude by considering the policy implications of clashes between states such as the US that have weaponized interdependence, and other states looking to counter these influences.

Statecraft and Structure: The Role of Global Networks

As globalization has advanced, it has fostered new networks of exchange – whether economic, informational or physical – that have remade domestic economies, densely and intimately interconnecting them in ways that are nearly impossible to unravel.[16] The financial

[16] 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

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 webpage can stitch together content and advertisements from a myriad of independently owned servers, which might be in the same city as the webpage's viewer, or on the other side of the world. Physical manufacture depends on vast tangled supply chains, which extend globally, vastly complicating trade wars, since raising tariffs on importers is likely to damage the interests of domestic suppliers.

The standard liberal story sees globalization as a fragmented and complex system that empowers new actors in ways that make it easier to achieve liberal objectives.[17] Most notably, scholars like Anne-Marie Slaughter claim that globalization creates decentralized networks that generate new opportunities for cooperative diplomacy.[18] Slaughter's guiding metaphor for globalization is a network of points resembling the multitudes of lights that one sees from a plane during a night landing. In such a network, an arbitrarily large number of paths may connect two or several of these points together, suggesting that globalization is best understood as a non-hierarchical 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,

---

reductionism similar to ours, see Thomas Oatley, "The Reductionist Gamble: Open Economy Politics in the Global Economy*." International Organization* Vol. 65, No. 2 (2011), pp. 311-341.
[17] See, for example Susan Strange, *The Retreat of the State: The Diffusion of Power in the World Economy* (New York: Cambridge University Press 1996), Philip Cerny, *Rethinking World Politics: A Theory of Transnational Pluralism* (New York: Oxford University Press 2010).
[18] Raustiala, "The Architecture of International Cooperation," Slaughter, *The New World Order* and *The Chessboard and the Web*.

liberals like Slaughter argue, power is "power with" – the power to work together constructively with allies, rather than "power over."[19]

Unfortunately for liberals, there is strong reason to believe that this understanding of globalization is radically incomplete. Cross-national networks, contrary to liberal claims, do not produce a flat or fragmented world of diffuse power relations and ready cooperation. Instead, they result in a specific and tangible configuration of power asymmetries. International commercial exchange – like many other complex phenomena – tends to generate heavily asymmetric networks in which exchange becomes centralized, flowing through a few specific intermediaries.[20] Rather than a random pattern of lights, economic interdependence produces structural relations like the 'hub and spoke' system that large airlines use to minimize transaction costs.

This 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 structures like the computers that run Internet exchanges or institutions such as a particular bank.

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

[19] Slaughter, *The Chessboard and the Web*.
[20] Judge, "Intermediary Influence".

business actors lead, inadvertently or otherwise, to highly centralized global networks of communication, exchange and physical production. Contrary to liberal claims, global economic and informational networks are often, and perhaps even typically highly asymmetric. This means that globalization – like other networked forms of human activity[21] – typically generates networks with stark inequality of influence.[22] The distribution of degree (e.g. of links across nodes) may approximate to a power law, or a log normal distribution, or a stretched exponential depending on particulars.[23] For the purposes of our argument, the exact statistical classification of the distributions is irrelevant – what *is* important is that social networks tend in general to be highly unequal in a variety of fashions.

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

[21] Newman and Park, "Why Social Networks." An important literature in statistical physics and related disciplines studies the topology of large scale networks, and how topology shapes e.g. processes of contagion. See Duncan Watts, "The 'New' Science of Networks," *Annual Review of Sociology* (2004), Vol. 30, pp.243-270 for a useful overview, and Mark Newman, Albert-László Barabási, and Duncan J. Watts (eds.), *The Structure and Dynamics of Networks*, (Princeton, NJ: Princeton University Press, 2011) for an excellent selection of important work. This literature has been underused by political scientists, who have focused on other aspects of networks, as in Emilie Hafner-Burton, Miles Kahler, and Alexander H. Montgomery. "Network Analysis for International Relations," *International Organization* (2009), Vol. 63, No. 3 , pp. 559-592. For an important exception, see Goddard, "Embedded Revisionism"

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

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

distributions are likely to emerge over time.[24] Network effects, in which the value of a service to its users increases as a function of the number of users already using it, may lead actors to converge on networks that already have many participants, while efficiency concerns lead the network providers to create hub-and-spoke systems of communication. Finally, innovation research suggests that there are important learning-by-doing effects, in which central nodes in networks have access to more information and relationships than other members of the network causing others to link to them preferentially to maintain access to learning processes.[25]

These mechanisms, and possibly others, 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 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.[26] Furthermore, under reasonable models of network growth, these topologies are self reinforcing – as the pattern starts to become established, new nodes become overwhelmingly likely to reinforce rather than to undermine the existing unequal pattern of distribution.

---

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

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

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

Nor are these just abstract theoretical claims. They appear to describe many global economic networks.[27] Even when global networks largely came into being through entirely decentralized processes, they have come to display high skewedness in the distribution of degree.[28] More plainly put, some nodes in these networks are far better connected than others. Studies of trade[29] and banking[30] show that the US and UK are exceptionally highly connected nodes in global financial networks. 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 display a similar skew towards nodes in advanced industrial democracies such as the US and (to a lesser extent) the UK.[31]

All this is driven by a primarily economic logic. In a networked world, businesses often operate in a context where there are increasing returns to scale, network effects, or some combination. This pushes markets towards 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.

---

[27] Thomas Oatley, W. Kindred Winecoff, Andrew Pennock, and Sarah Bauerle Danzman. "The Political Economy of Global Finance: A Network Model," *Perspectives on Politics* Vol. 11, No. 1 (2013), pp.133-153, Oatley, Thomas, *A Political Economy of American Hegemony* (New York: Cambridge University Press 2015).

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

[29] Giorgio Faviolo, Javier Reyes, and Stefano Schiavo, "World-Trade Web: Topological Properties, Dynamics, and Evolution," *Physical Review E* Vol. 79, No. 3 (2009), pp. 036115-1-19, Luca De Benedictis and Lucia Tajoli, "The World Trade Network," *The World Economy* Vol. 34, No. 8 (2011), pp. 1417-1454.

[30] Thomas Oatley et al., "The Political Economy of Global Finance," William Kindred Winecoff, "Structural Power and the Global Financial Crisis: A Network Analytical Approach," *Business and Politics* Vol. 17, No. 3 (2015), pp. 495-525.

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

Even where networks are run by non-profit actors, there are strong imperatives towards network structures in which most or even nearly all market actors work through a specific organization, allowing them to take advantage of the lower transaction costs associated with centralized communications architectures.

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

For example, Facebook's business model is centered on monetizing individuals' social networks through targeted advertisement and other means. It has been able to resist challengers with 'better' or less privacy invasive products, because it is relatively costly for an individual, or even a small group to move to a different service unless they know that everyone else is doing the same thing. Google similarly looks to leverage the benefits of search and advertising data.[32] Large international banks such as Citibank, security settlement systems such as Euroclear, consumer credit payment systems such as Visa/Mastercard, financial clearing houses such as CHIP, and financial messaging services such as SWIFT have become crucial intermediaries in global financial networks, acting as middlemen across an enormous number and variety of specific transactions. All these play key roles in their various architectures, coordinating and brokering enormous numbers of specific relationships, benefiting from the efficiencies of scale

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

that this allows, and in some cases from the unique access to information that their brokerage position provides them with.[33]

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

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

New Forms of Network Power: Panopticons and Choke points

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. However, 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,

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

structures that were generated by market actors in pursuit of efficiency and market power can be used by states for their own quite different purposes.

Here, we differentiate our argument about network structure from two related but distinct sources of power that may result from economic interdependence. The first is market power. While 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 GDP) of a country. States with large economic markets can leverage market access for strategic ends. National economic capabilities, then, produce power resources.[34] The second, which dates back to the pioneering work by Keohane and Nye (1977) and has been most thoroughly examined in the case of trade, emphasizes the power generated by bilateral dependence. States, which rely on a particular good from another state and lack a substitute supplier, may be sensitive to shocks or manipulation.[35]

Market size and bilateral economic interactions are important, but far from exhaustive of the structural transformations wreaked by globalization. Global economic networks have distinct consequences that go far beyond states' unilateral decisions to allow or deny market access, or imposition of bilateral pressure. They allow some states to weaponize interdependence on the level of the network itself. Specifically, they enable two forms of weaponization. The first weaponizes the ability to glean critical knowledge from information flows. This creates a public

[34] Shambaugh, George E. "Dominance, Dependence, and Political Power: Tethering technology in the 1980s and today." *International Studies Quarterly* 40.4 (1996): 559-588; Simmons, Beth A. "The international politics of harmonization: the case of capital market regulation." *International Organization* 55.3 (2001): 589-620; Daniel Drezner, *All Politics is Global*. Princeton: Princeton University Press. 2007.

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

authority analogue to learning-by-doing, which we label the *panopticon effect*. 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. Since 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 worked in earlier periods of globalization as it did today. As Harold James describes it, "in the first era of globalization, expanding trade, capital and labour flows all tied economies together in what appeared to be an increasing and probably irreversible network," centered on the "commercial infrastructure provided by Britain," and in particular the financial infrastructure of the City of London.[36] 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.[37]

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

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

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

Such information offers privileged states a key window into the activity of adversaries, compensating for the weak information environment that is otherwise common in global politics. As a result, states with access to the panopticon effect have an information advantage in understanding adversaries' intentions and tactics. This 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 *choke point effect*, and involves privileged states' capacity to limit or penalize use of hubs by third parties (e.g. other states or private actors). Because hubs offer extraordinary efficiency benefits, and because it is extremely difficult to circumvent them, states that can control hubs have considerable coercive power, and states or other actors that are denied access to hubs can suffer very substantial consequences.

States may use a range of tools to achieve choke point effects. This allows us to situate existing research findings in both international political economy and international security on states' extraterritorial power.[38] In some cases, states have direct 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 them to work together with others to

[38] Kaczmarek, Sarah C., and Abraham L. Newman. "The long arm of the law: Extraterritoriality and the national implementation of foreign bribery legislation." *International Organization* 65, no. 4 (2011), pp. 745-770; Raustiala, Kal. *Does the constitution follow the flag?: the evolution of territoriality in American law*. Oxford University Press, 2011; Putnam, Tonya L. *Courts without borders: Law, politics, and US extraterritoriality*. Cambridge University Press, 2016.

exploit the benefits of coercion. The existing literature on sanctions discusses how statecraft, credibility, the ability to involve allies and other such factors shape the relative success or failure of coercive policies. Our account, in contrast, highlights the crucial importance of the network structures within which all of these coercive efforts take place. Where there are one or a few hubs, it becomes far easier for actors in control of these nodes to block or hamper access to the entire network.

Our account explains 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 activate the network structure. First, only those states, which have physical or legal jurisdiction over hub nodes, will be able properly to exploit the benefits of weaponized interdependence. As we have already noted, the network hubs of globalization are not scattered at random across the world. Instead, they are disproportionally located in the advanced industrial countries, in particular the United States, which has led technological and market innovation in the most recent round of economic globalization. This effectively means that only the US and a couple of other key states (most notably the European Union and, increasingly, China) enjoy the benefits of weaponized interdependence, although others (as we discuss below) 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 not have this at all, or alternatively may only be able to prosecute strategies based on panopticon effects rather than chokepoints, or vice versa. The literature on regulatory capacity, for example, demonstrates that the United States is not uniformly positioned to control market

access.[39] 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 choke point effects.

In other domains, states may be constrained by national laws and norms from engaging in certain kinds of weaponization. Privacy laws in the European Union, for example, limit the amount of data that may be collected or stored by commercial internet providers. These institutions, which were adopted just as decentralized market processes generated new commercial networks of data exchange, mean that it is more difficult for many European governments to directly exploit panopticon effects. As history demonstrates, domestic institutions may change in response to new perceived threats,[40] but they may also be sticky, since domestic actors may fear that the new capacities will be turned against them as well as foreign adversaries.

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 choke point effects. Variation in domestic institutions in terms of capacity and key norms may limit their ability to use these coercive tools even when states have territorial or

---

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

[40] Henry Farrell and Abraham Newman, *Of Privacy and Power*.

jurisdictional claims over hubs. Where control over key hubs is spread across a small number of states, these states may need to coordinate with each other to exploit weaponized interdependence. States, which 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 US – were able to take advantage of these network structures, to exploit panopticon effects or choke point effects. Importantly, our cases offer variation in the ability of the US to deploy these strategies, distinguishing our argument from more conventional market power or bilateral vulnerability accounts.

The Rise of Network Inequality

While globalization is often characterized as involving complexity and fragmentation, this section demonstrates how in a range of issue areas – finance and information – strong systematic inequalities have emerged. In particular, these narratives demonstrate how market actors created institutions and technologies to overcome the transaction costs associated with market 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 in order to move funds from one entity to another. A key component of the payment system, then, is a reliable and secure system that allows financial institutions to communicate with one another regarding the multitude of transactions that occur globally on any given day.

Since the 1970s, this has been provided by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[41] For much of the post-war 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 provided by national telecommunications providers. These systems proved both incredibly slow and insecure. These inefficiencies led financial actors to create a number of competing platforms for inter-bank communication in the 1970s. Most notably, the First National City Bank (FNCB) of New York developed a proprietary system known as Machine Readable Telegraphic Input (MARTI), which the company hoped to disseminate and profit from.

This gave a big push to European banks and US competitors of FNCB, who worried about what might happen if they became dependent on the MARTI system. The result was that a small group of European and US banks to cooperate in building a messaging system that could

[41] Our history of SWIFT in this section relies extensively on Susan V. Scott and Markos Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community* (London: Routledge, 2014). SWIFT is remarkably understudied by international security scholars, considering its empirical importance to sanctions. For a key exception, see Erik Jones, and Andrew Whitworth. "," *Survival* Vol. 56, No. 5 (2014), pp. 21-30. For discussions of SWIFT in the EU-US relationship, see Marieke De Goede, "The SWIFT Affair and the Global Politics of European Security," *Journal of Common Market Studies* Vol. 50, no. 2 (2012), pp. 214-230; Henry Farrell and Abraham Newman, "The New Politics of Interdependence: Cross-National Layering in Trans-Atlantic Regulatory Disputes," *Comparative Political Studies*, Vol. 48, No. 4 (2015), pp. 497-526.

replace the public providers and speed up the payment process. SWIFT opened its doors in 1973 and sent its first message in 1977.

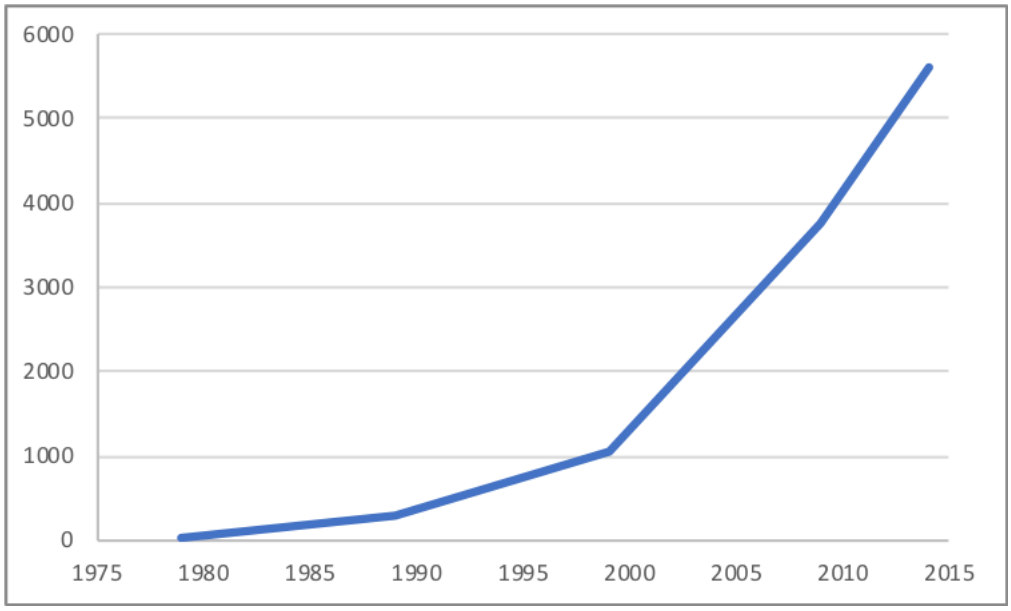
The main objective of the body was to create a system for transferring the payment instructions between entities engaged in a financial transaction including banks, settlement institutions, and even central banks. SWIFT plays a critical role in authorizing transactions, authenticating parties, and recording exchanges. It is a cooperative run by representatives from the different financial institutions involved. SWIFT's headquarters was located in 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 500 firms with an annual traffic of just over 3000 messages. By 2016, it had become the dominant provider serving more than 200 countries and some 11,000 financial institutions, communicating over 6.5 billion messages annually. As Scott and 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."[42] This network effect was an accidental rather than an intended outcome. Those involved in the original SWIFT project during the 1970s were solely focused on "creating an entity, a closed society, to bind members together in an

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

organizational form that would employ standards designed to create efficiencies on transactions between the member banks".[43]

Figure 1: Annual SWIFT Messages in Millions



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

[43] P.107, Scott and Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication.*

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.[44] By the turn of the millennium nearly all major global financial institutions used the SWIFT system to process their transactions.

The Internet – All roads lead through Northern Virginia

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

> that would inter alia require the licensing of journalists, enhanced abilities for governments to keep out unwanted transmissions of news and other information, and a "balanced" flow of information between the global North and South.[45]

This led to OECD discussions about whether "trans-border data flows" posed a problem for national sovereignty.[46] The US government and US businesses looked to divert this debate,

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

ensuring that the final OECD Declaration in 1985 called on governments "to avoid the creation of unjustified barriers to the international exchange of data and information."[47] Proposals for a wide-reaching set of international institutions fell by the wayside. Instead the OECD principles were non-binding and primarily focused on questions of privacy, where the US and EU member states came to loose agreement in principle, without agreeing on whether the instruments should have teeth. While these disagreements were taking place, technical experts, who were primarily interested in the best ways of sharing scarce computer resources within the US research and military establishment, developed technical protocols for 'packet switching' into the TCP/IP protocols that, in modified form, remain the cornerstone of the Internet today. The Internet spread internationally, but primarily within a specialized technical community, so that e.g. national top level domain names were effectively allocated by a single individual, Jon Postel, to persons or organizations that seemed trustworthy.

When the Internet came to public prominence in the early 1990s, it initially seemed as though it might provide a technology that was innately resistant to centralization. Authorities and political actors including US President Bill Clinton believed that it was effectively invulnerable to central control.[48] In contrast to 'centralized' networks such as the then existing phone system, where different phones connected through a central switchboard, the Internet was conceived as a 'distributed' network, where there was a multiplicity of links between different nodes, and no

[47] P.51, William J. Drake, "Introduction," William J. Drake and Ernest J. Wilson (eds), *Governing Global Electronic Networks: International Perspectives on Policy and Power* (Cambridge MA: The MIT Press, 2008).
[48] William J. Clinton, *Remarks at the Paul H. Nitze School of Advanced International Studies*, Washington DC, Johns Hopkins SAIS, March 8, 2000. http://www.presidency.ucsb.edu/ws/?pid=87714.

node was significantly more important than any other.[49] The TCP/IP protocol allowed servers to speedily identify blockages in the system and find alternative routes for information. In such a system, government control seemed very difficult – as the prominent activist John Gilmore put it, the "Net interprets censorship as damage, and routes around it."[50] This led some online libertarians to forecast the withering of the state and a new age of human freedom.[51]

Contradicting these heady prognoses, the underlying architecture of the Internet became increasingly centralized over time.[52] Some hubs and interconnections between these hubs became far more important than others. States increasingly were able to impose controls on traffic entering and leaving their country, while censoring or controlling many ordinary uses of the Internet.[53] 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. The vast majority of global Internet traffic travels across roughly 300 cables. There are fewer than a half dozen cables directly connecting Western Europe and Africa. The importance of these central communication nodes became painfully clear in 2008, when a ships anchor severed two such cables (FLAG Europe Asia and SEA-ME-WE-4) off the cost of Egypt and shut

---

[49] On the theory of distributed networks, see Paul Baran, "On Distributed Communications Networks," IEEE Transactions on Communications Systems Vol. 12, No. 1 (1964), pp.1-9.
[50] Philip Elmer-Dewitt, "First Nation in Cyberspace," *Time Magazine*, December 6, 1993. http://content.time.com/time/magazine/article/0,9171,979768,00.html.
[51] John Perry Barlow, "A Declaration of the Independence of Cyberspace." *The Humanist* Vol. 56, No. 3 (1996), p 18.
[52] Albert, Jeong, and Barabási. "Internet: Diameter of the World-Wide Web."
[53] Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006), Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Janice Gross Stein. *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: The MIT Press, 2008), Adam Segal, *The Hacked World* Order (New York, NY: Public Affairs 2017), Joshua A. Tucker, Yannis Theocharis, Margaret E. Roberts, and Pablo Barbera (2017), "From Liberation to Turmoil: Social Media and Democracy," *Journal of Democracy*, Vol. 28, No.4, pp.46-59.

down much of the Internet in the Middle East and South Asia. This problem has reoccurred, leading public officials to raise concerns about vulnerability to sabotage.[54]

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.[55] These Internet exchanges are often located in major cities and channel the majority of domestic Internet traffic in the United States and Europe, as well as supporting peer linkages between the different global networks that allow the Internet to function. Once again, this means that a very large amount of traffic travels through a few dozen points.

Network economies have similarly led to a centralization of the e-commerce economy, as both network effects and new kinds of increasing returns to scale cemented the global dominance of a very small number of e-commerce companies. This is in part thanks to US government policy. The US believed that to the greatest extent possible, data governance should involve the free flow of content across borders (except, of course, where this interfered with the intellectual property or other interests of US corporations). It should furthermore be based primarily on self-regulation, looking to business cooperation and market structures to regulate their relations with consumers.[56]

---

[54] Chris Baynes, "Entire Country Taken Offline for Two Days after Undersea Internet Cable Cut," *Independent*, April 10 (2018); Arj Singh, "Russia 'could cut UK's undersea internet cables', defence chief warns," *Independent*, December 14 (2017)

[55] See Patrick S. Ryan and Jason Gerson. "A Primer on Internet Exchange Points for Policymakers and Non-Engineers," *Social Science Research Network* (2012). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2128103, Kuai Xu, Zhenhai Duan, Zhi-Li Zhang, and Jaideep Chandrashekar, "On Properties of Internet Exchange Points and Their impact on AS Topology and Relationship." In *International Conference on Research in Networking*, pp. 284-295. Springer, Berlin, Heidelberg, 2004.

[56] Author Interview with Ira Magaziner, New York, September 21, 2000.

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.[57] The US government scotched plans by Postel to set up a global institution to regulate the Internet with the help of the Internet Society and the UN's International Telecommunications Union, threatening him with criminal sanctions if he did not back down.[58]

Instead, it handed authority over domain names to a private non-profit corporation under Californian law, the Internet Corporation for Assigned Names and Numbers (ICANN), which would work together with for profit entities to manage the technical aspects of coordination.[59] ICANN's ultimate authority stemmed from a contract with the Department of Commerce – this provided the US with a controversial implicit veto. Importantly, however, ICANN was designed according to a 'stakeholder' model, under which private actors would take the lead in shaping its deliberations. The US veto was a backstop against other states or international organizations wresting ICANN away from the private sector, rather than a calibrated tool for institutional interference.

Self regulation and individual choice were also the organizing principles for US domestic regulations. The cornerstone of this regime was a principle laid out in legislation including most

[57] United States White House Office, *A Framework for Global Electronic Commerce* (Washington, DC: White House, 1997).
[58] Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge MA: The MIT Press 2009).
[59] Mueller, *Ruling the Root.*

importantly Section 230 of the Communications Decency Act - the lack of "intermediary liability" for e-commerce firms that allowed others to put up content.[60]

This was intended for a specific and relatively narrow purpose – to provide businesses with safe harbor against legal actions that were aimed at content posted by users. It ended up inadvertently reinforcing a new business model, in which e-commerce firms, rather than providing content themselves, would rely on their users to provide the content for them. They could then make their profits by acting as an intermediary between those users, analyzing their behavior, and offering targeted advertising services to their actual customers, people who wanted to sell products to the users leaving data trails behind them. Because these businesses were not liable for the individual activities of their users they could potentially scale quickly and massively, relying on algorithms rather than human beings to manage their users, run marketplaces for their customers, and monitor their content (e.g. for copyright violation under the 'notice and takedown' system that US law facilitated).

This, together with network effects, led to the rapid domination of a small number of e-commerce and online companies. Companies like Facebook and YouTube (owned by Google and then by Alphabet) were able to use the lack of intermediary liability to rapidly scale up, allowing billions or hundreds of millions of users respectively to share content, without any need 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. [61] Google could similarly take advantage of the lack of intermediary liability, while expanding out into new services, and reaping the benefits of a feedback loop in which its users inadvertently

[60] Jack M. Balkin, "The Future of Free Expression in a Digital Age," *Pepperdine Law Review* Vol. 36 (2008), pp.427-444.
[61] See more generally, Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

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, not only selling physical products, but cloud services, and acting as an intermediary across a wide variety of markets.

All of these firms built themselves effective near monopolies. Facebook – once it had become established – was more or less impossible for competitors to take down, since its users had little incentive to migrate to a new system, and Facebook was capable of buying and integrating potential new competitors long before they could become real threats. Google's control both of data and the means to analyze it, provided it with a nearly impregnable position, while Amazon's relentless growth into new marketplaces provided it with irresistible economies of scale.[62]

Although some countries, such as China have largely excluded these companies and developed domestic competitors, they have only done so by leveraging state power in ways that are far harder for weaker states and liberal democracies. As a result, a huge fraction of global data traffic is channeled through the servers of a small 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.[63] Furthermore, as more and more online services move to cloud architectures, which store customer data and processing power in online data centers, cloud providers have emerged as central hubs.[64] One estimate, for example, suggests that 70 percent of global web traffic goes through Amazon Web Services in Northern

[62] Khan, "Amazon's Anti-Trust Paradox."
[63] See Laura DeNardis, "Hidden Levers of Internet Control," *Information, Communication and Society*, Vol. 15, No. 5, pp. 720-738; Tusikov, *Chokepoints*.
[64] Bruce Schneier, "Censorship in the Age of Large Cloud Providers," *Lawfare*, June 7 2018. https://lawfareblog.com/censorship-age-large-cloud-providers.

Virginia (which had become established as a hub location earlier thanks to America Online).[65] Thus, transcontinental fiber optic cables, Internet exchanges, monopoly service providers and geographically concentrated datacenters 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 US, and channel the vast majority of global data exchanges.

Weaponizing the Hubs

With the rise of these central hubs across the issue areas, states (and in particular the US and the European Union) began exploring how they could exploit network properties to weaponized interdependence. In what follows, we use the case-evidence to demonstrate the two forms of network power – panopticon and choke point effects – and explain variation in their use. In particular, the case of financial messaging underscores the importance of institutional capacity and differences between the US and Europe in their ability to activate these strategies. The case of the Internet underscores how domestic institutions and norms constrain US behavior even when it has physical and legal jurisdiction over key hubs.

SWIFT, Counter-Terrorism and Non-Proliferation

SWIFT demonstrates how both the panopticon and choke point effects can work. Because SWIFT is central to the international payment system, it both provided data about the vast majority of global financial transactions and allowed these transactions to take place. For the last 25 years, key states, most importantly the US, have gradually transformed the repository of

[65] Benjamin Freed, "70 Percent of the World's Web Traffic Flows through Loudoun County," *Washingtonian*, September 14 2016.

transfers into a surveillance asset and financial sector dependence into a tool of asymmetric interdependence.

Although the attacks of September 11th were a crux point for global surveillance, governments began considering SWIFT's potential much earlier. In fact, the Financial Action Task Force (FATF), which is a core global governance body focused on anti-money laundering with an early focus on organized crime and drug trafficking approached SWIFT in 1992.[66] FATF hoped to gain access to SWIFT records so as to track down illicit activity. It was at this point that SWIFT realized the peril of the economic efficiencies that it itself had created. As Lenny Schrank, former chief executive 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."[67] SWIFT refused the request, claiming that it was not able to provide information to public authorities and that such requests had to be directed to banks and other financial institutions engaged in a transaction. The organization claimed that it was a communications carrier much like a telephone operator rather than a data processor and thus should be immune to government monitoring.

SWIFT kept governments at bay for much of the 1990s, but succumbed after the attacks of September 11 2001.[68] In the wake of the attacks, the United States government led by the US Treasury began to examine ways to use the global financial system to curtail terrorist financing,

---

[66] On FATF, see Eleni Tsingou, "Global Financial Governance and the Developing Anti-Money laundering regime: What Lessons for International Political Economy?," *International Politics*, Vol. 47, No.6 (2010), pp.617-637, Anne L. Clunan, "The Fight Against Terrorist Financing," *Political Science Quarterly* Vol 121, No. 4 (2006-2007), pp. 569-596.
[67] P. 128, Scott and Zachariadis, *The Society for Worldwide Interbank Financial Telecommunication.*
[68] See Caytas, "Weaponizing Finance", pp.441-475 for an excellent overview of both SWIFT and the dollar clearing system.

targeting the terrorist money supply, and concluded that it could lawfully issue enforceable subpoenas against SWIFT to compel it to provide financial data. This Treasury initiative became known as the Terrorist Finance Tracking Program (TFTP).[69] In this effort, the Treasury quickly came to target SWIFT as a key channel to accomplish this end. It was especially hard for SWIFT to resist Treasury demands, because the organization maintained a mirror data center containing its records in Virginia. In the years that followed, SWIFT secretly served as a global eye for the US fight against terrorism, with the Treasury department able to use the SWIFT system to monitor and investigate illicit activity.[70] As Juan Zarate, a former treasury department official explained:

> Access to SWIFT data would give the US government a method of uncovering never-before-seen financial links, information that could unlock important clues to the next plot or allow an entire support network to be exposed and disrupted.[71]

The SWIFT data became the 'Rosetta stone' for US counter-terrorism operations as it shed light on the complex networks of terrorist financing. The government used the data as a key forensic tool to identify terrorist operations, co-conspirators and planning. This effort became so central to US and European counter-terrorism operations that when it was challenged by civil-liberties-oriented actors in Europe, the US government employed top officials including

---

[69] Farrell and Newman, "The New Politics of Interdependence."; https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx

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

[71] Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (London, UK: Hachette 2013).

Secretary of State Hillary Clinton and Secretary of the Treasury Timothy Geithner to defend and demand the continuation of the program. As one EU foreign minister concluded, "they pulled out all the moral and political stops".[72] 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".[73] Despite initial public protests, the dominant coalition in EU politics quietly approved of the US use of SWIFT to create a financial data panopticon, so long as the US was prepared to share the proceeds.[74]

Efforts to weaponize SWIFT were not limited to the panopticon effect. As Joanna Freytas notes:

> The most vulnerable element of financial infrastructure is its payments system, both at a national (macro) level and on an institutional (micro) plane. … 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.[75]

[72] Hans-Jürgen Schlamp, "EU to Allow US Access to Bank Transaction Data," *Spiegel Online*, November 27 (2009).
[73] European Commission, *Joint Review Report of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the Untied States for the purposes of the Terrorist Finance Tracking Program*, SWD(2017) 17 final. European Commission: Brussels (2017).
[74] Farrell and Newman, "The New Politics of Interdependence."
[75] pp.449-51, Caytas, "Weaponizing Finance."

As an example of the power of chokepoints, US and European policy-makers used SWIFT to reinforce the sanctions regime against the Iranian regime. Starting in the 2000s, a group of prominent US policy-makers led by Ambassadors Richard Holbrook and Dennis Ross started a private campaign, known as United Against Nuclear Iran (UANI), to ratchet up pressure on the Iranian regime. The group targeted SWIFT as complicit in assisting the Iranian regime and contributing to its economic health.[76] As per SWIFT's 2010 annual report, some 19 Iranian banks as well as another 25 institutions relied on the messaging system.[77] 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."[78]

This campaign had consequences in both the US and Europe. On February 2 2012, the US Senate Banking Committee adopted language that would have allowed the US government to sanction SWIFT if it continued to allow Iranian financial institutions to use the SWIFT system, pushing the administration to adopt a more pro-active stance.[79] The European Union, followed up on this threat in March both because of US pressure and its own worries about Iran's nuclear

[76] United Against Nuclear Iran, *SWIFT Campaign* (Washington DC: UANI 2012).
[77] SWIFT, *Annual Review 2010: Common Challenges, Unique Solutions*, SWIFT: Brussels (2010).
[78]UANI Letter to SWIFT, January 30, 2012. https://www.unitedagainstnucleariran.com/sites/default/files/IBR%20Correspondence/UANI_Letter_to_SWIFT_013012.pdf; Jay Solomon and Adam Entous, "Banking Hub adds to Pressure on Iran," *Wall Street Journal*, February 4 (2012).
[79] Jay Solomon, *The Iran Wars: Spy Games, Bank Battles, and the Secret Deals that Reshaped the Middle East* (New York: Random House 2016).

program, passing regulations that prohibited financial messaging services (e.g. SWIFT) from providing services to targeted institutions.[80]

The combination of EU and US 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.[81] As Lazaro Campos, former CEO 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."[82]

The Iranian regime quickly felt the SWIFT noose tighten as its major financial institutions, including its central bank, found themselves locked out from the international payment system. As explained by a EU official at the time, "It is a very efficient measure…It can seriously cripple the banking sector in Iran".[83] Unwinding the SWIFT measures became a key bargaining point in the negotiations over Iran's nuclear program.[84] During the P5+1 negotiations, 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, 'on whether the United States wants to lift the sanctions or keep them.' [85]Accordingly, a lifting of the SWIFT measures was a key part of the eventual JCPOA deal.

---

[80] Agence France Presse, "US presses EU to close SWIFT network to Iran," February 16 (2012); Samuel Rubenfeld, "SWIFT to Comply with EU Ban on Blacklisted Entities," *Wall Street Journal*, March 15 (2018).
[81] Arnold, "The True Cost of Financial Sanctions."; Associated Press, "Iran cut off from Global Financial System," March 15 (2012).
[82] SWIFT press release, March 15 2012. https://www.unitedagainstnucleariran.com/index.php/swift.
[83] 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).
[84] Zarate, *Treasury's War*.
[85] P. 85, Arnold, "The True Costs of Financial Sanctions."

Notably, the SWIFT measures were a result of joint pressure from both of the jurisdictions that it was substantially exposed to. Had the US not imposed pressure, it is unlikely that the EU 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.[86] Equally, however, the US might have had difficulties in acting unilaterally in the face of concerted EU opposition, given SWIFT's primary location in Europe. This dynamic is playing out as the US administration has backed out of the JCPOA, threatening to reimpose SWIFT restrictions on Iran, while the European Union resists the re-weaponization of SWIFT.[87]

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 choke point effects, just as our framework predicts. Furthermore, the topology and existence of the global financial network provided the US (and 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 US and EU could only have unilaterally denied access to their own markets, or invoked

[86] Caytas, "Weaponizing Finance."
[87] Sam Fleming, Philip Stafford and Jim Brunsden, "US and EU Head for Showdown over Shutting Iran off from Finance," *Financial Times*, May 17 (2018); Richard Goldberg and Mark Dubowitz, "To Help Iran, Angela Merkel Tries to Pull a Fast one with SWIFT," *Wall Street Journal*, June 20 (2018).

bilateral dependencies to squeeze their adversaries, they would have been far less effective, since adversary states could readily have turned to other financial partners.

The NSA, PRISM and Counter-terrorism

The US enjoyed similar – and arguably even greater – dominance over information networks and e-commerce firms, thanks to asymmetric network structures. However, it was far less eager to deploy the chokepoint effect. This reflected strategic calculation of benefits – the US believed that a general diffusion of communication technology and the global dominance of US e-commerce firms was in its interests. It also reflected domestic institutional constraints. The US had effectively pre-committed to keeping e-commerce free from government control, except for truly compelling problems such as child pornography. This 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 tradeoffs. Thus, for example, the US sanctions regime applied to technology companies as well as other commercial actors, but the US created specific (if dubiously beneficial) carveouts that were intended to allow technology companies to support openness in Iran and other regimes subject to US sanctions.[88]

The US, under the Clinton, Bush II and Obama administrations, saw the spread of Internet openness as linked to the spread of democracy, and thus strategically beneficial for the US, as well as reflecting US values.[89] In a much remarked upon major speech, Secretary of State

[88] See Daniel Kehl, "US Government Clarifies Tech Authorizations under Iranian Sanctions," *New America*, February 14, 2014.
[89] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York, NY: Basic Books); Daniel McCarthy, "Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet," Foreign Policy Analysis Vol.

Hillary 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."[90] If the US 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 US influence. Thus, the US largely refrained from overt pressure on e-commerce firms to help it achieve specific political outcomes. In one exceptional instance, a US official asked Twitter to delay a temporary technical shutdown in the middle of the 2009 protests in Iran, on the mistaken belief that Twitter was playing an important part in helping organize the protests.[91] The action was controversial, and was not publicly repeated. The US 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."[92]

Finally, the US 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 US pushed back forcefully.[93] Renewed pressure in 2012 combined

---

7, No. 1 (2011) pp.89-111; Ryan David Kiggins, "Open for Expansion: US Policy and the Purpose for the Internet in the Post-Cold War Era," International Studies Perspectives Vol. 16, No. 1 (2015), pp.86-105.

[90] Hillary Rodham Clinton, *Remarks on Internet Freedom*, Washington DC, January 21, 2010.

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

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

[93] Segal, *The Hacked World Order.*

with the Snowden revelations to put the US in a more awkward position – it finally accepted that ICANN needed to be separated from the US government, and internationalized ICANN in the closing days of the Obama administration.[94]

Even while the US declined to use chokepoints and promoted the cause of an open Internet, it took enormous advantage from the panopticon effect. The concentration of network hubs and e-commerce firms within the US offered extraordinary benefits for information gathering, which the US was swift to take advantage of, especially after the September 11 attacks. After September 11, 2001, the US quickly moved to leverage this advantage through the STELLARWIND program, which caused some consternation within the Bush administration, and was eventually found by the Office of Legal Council to be illegal. However, it was soon replaced by a variety of other programs designed to take advantage of the US's unparalleled location at the heart of global networks of information exchange. In the blunt description of former NSA Director Michael Hayden:[95]

> 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?

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

In some cases, the US was able to do this through publicly undisclosed direct relations with technology companies. Michael Hirsch describes how technology companies were simultaneously worried about being seen as "instruments of government" but willing to recognize that they needed to cooperate with the government on key issues.[96] Under the PRISM program, the US had substantial legal authority to compel the production of records and information regarding non-US individuals from technology companies.

In addition, the US demanded the cooperation of telecommunications companies in carrying out "upstream collection" of large amounts of data from US companies such as AT&T that help run the Internet backbone.[97]

> According to the NSA's documents, it values AT&T not only because it "has access to information that transits the nation," but also because it maintains unique relationships with other phone and internet providers. The NSA exploits these relationships for surveillance purposes, commandeering AT&T's massive infrastructure and using it as a platform to covertly tap into communications processed by other companies.

The US can copy data in bulk and mine it later for valuable information, while facially complying with US laws that distinguish between the data of US and non-US citizens ('incidental collection' of data on US citizens is permissible). [98] It has gathered data from

[96] Hirsch, "America's Top Companies."
[97] Ryan Gallagher and Henrik Moltke "The NSA's Hidden Hubs in Eight US Cities," *The Intercept* (June 25, 2018); Marcy Wheeler, "Verizon Gets Out of the Upstream Surveillance Business," *Emptywheel.com*, May 6, 2017.
[98] For comprehensive descriptions of the various US electronic surveillance programs, see Laura K. Donohue, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age* (New York: Oxford University Press, 2016), and Jennifer Stisa Granick, *American Spies:*

Internet exchange points, and from the cable landing stations where undersea cables reach dry land. This provided it with an alternative source of information to PRISM, and also gave it direct reach into the internal data of US e-commerce firms without their knowledge and consent, tapping for example, into the communication flows through which Google reconciled data in different countries.

The release of documents by Edward Snowden, a former NSA contractor, in 2013, US monitoring provoked political uproar, both in the US and elsewhere. The result was a series of legal reforms that partly limited US government access to the data of US citizens, as well as policy measures including a Presidential Policy Directive intended to reassure allies that the US would not use their citizens' information in unduly invasive ways.[99]

Other states certainly engaged in surveillance activities, including members of the European Union (European privacy law does not currently prevent external surveillance for espionage, including European countries spying on each other, although it does restrict the ability of states to retain data on their own citizens). However, they lacked the 'home advantage' of network centrality that Hayden referred to, and were correspondingly less able to gather useful information, with the consequence, for example, that America's European allies relied heavily on US willingness to share surveillance data for their own security.[100]

The Internet has regularly been depicted, both in the scholarly literature and in US political debate, as a fundamentally liberal space characterized by open exchange and cooperation. This rhetoric serves to conceal the power relations that shape the relationship

---

Modern Surveillance, Why You Should Care, and What to Do About It (New York: Cambridge University Press 2017). Many of the legal interpretations that allow US surveillance are still unknown, as are the details of key programs.

[99] (Farrell and Newman, forthcoming).

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

between the US and online communications networks. For sure, the US 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*.[101] Yet the US 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 that a state like the US could take advantage of, or where states were limited to employing the tools of national markets and bilateral pressure.

Conclusion

There is a common caricature in the literature on globalization, which suggests that greater economic exchange has fragmented and decentralized power relations. In this article, in contrast, we have argued that these economic interactions generate new structural conditions of power. This allows us to bring together the literature on security, which has paid deep and sustained attention to the systemic aspects of power, with the literature on global markets, which has largely neglected it. Empirically, we show how decentralized patterns of economic exchange have led to centralized global networks such as SWIFT and the Internet. Similar patterns prevail in other global networks such as the dollar clearing system. Theoretically, our account shows how the topography of networks has consequences for power relations, generating systematic differences in the coercive authority enjoyed by some states and not others. Bringing these together, our article provides a historically detailed account (a) of how the new network

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

structures that shape power and statecraft have come into being, (b) how these structures have been used to weaponize interdependence by privileged actors (who possess both leverage over network hubs and the appropriate domestic institutions that allow them to exercise this leverage).

Our study has far reaching implications for the study of international affairs. For scholars of economic interdependence and security studies, our argument seeks to bring the two into closer dialogue with each other and in doing so generating important new insights for both. On the one hand, we force IPE scholars 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 research on international security to consider how economic globalization may fundamentally transform the international structure and thus generate new forms of state power.

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

Our evidence from the cases of financial and digital communication furthermore offer important support for our theoretical claims. States need *both* leverage over network hubs *and* appropriate institutions if they are to take advantage of the panopticon and chokepoint effects. States and jurisdictions that have potential leverage over network hubs, but do not have the appropriate institutions, cannot make good use of weaponized interdependence. Thus, the European Union has fragmented instruments of financial regulation, which mean 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 US. Lacking a regulator like the Treasury Department's OFAC, or legal instruments like those that the US 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 US has. However, while we do not discuss it here, other research indicates that the EU is perfectly capable of leveraging market access in other domains where it has both influence over key hubs and well developed institutions (e.g. in the area of privacy).

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

Our framework also suggests that there are broader limits to weaponized interdependence. Most importantly, not all markets rest directly on asymmetric networks. For example, international oil markets are sufficiently diversified that they are relatively liquid, and thus present no single point of control.[102] Where there are no asymmetric networks, 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 either information gathering or the threatened or actual use of choke points.

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

We have now entered into a new stage, 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 who 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. Hence, the more that privileged states look to take advantage of their privilege, the more that other states and non-state actors will take action that might potentially weaken or even undermine the interdependent features of the pre-existing system.[103] The ability of states to resist weaponized interdependence will reflect, in part, their degree of autonomy from those economic interests that seek to maintain the benefits of centralized exchanges even in the face of greater constraints on state authority.

The US 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 position in the network. They highlight the importance of network structure, and the fact that these network structures are not immutable. States are locked into existing network structures only up to that point where the costs of remaining in them are lower than the benefits, and should this change, we may see transitions to new arrangements.

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

Thus, for example, the initial US decision to exclude Chinese firm ZTE from global supply chains appears to have precipitated a major reconsideration on the part of the Chinese government of China's reliance on foreign chip manufacturers, and the need for China to create its own domestic manufacturing capacities to mitigate its economic vulnerabilities.[104] Similar concerns led to initial US suspicion of Huawei and ZTE, and fears that their telecommunications equipment may have built-in vulnerabilities to assist Chinese surveillance. More weaponized interdependence may cause global supply chains to unravel.

Western threats to weaponize SWIFT against Russia in the wake of the Ukraine crisis produced similar responses. [105] 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."[106] In a major foreign policy speech, 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

---

[104] Henry Farrell and Abraham Newman, "Trump's U-Turn on Chinese Mega-Firm ZTE Damages U.S. Power and Credibility," *Washington Post* May 14, 2018.
[105] Gideon Rachman, "The Swift way to Get Putin to Scale Back His Ambitions," *Financial Times*, May 12, 2014. https://www.ft.com/content/d6ded902-d9be-11e3-920f-00144feabdc0; Economist staff writers, "Too smart by Half?: Effective Sanctions Have Always Been Hard to Craft," *The Economist*, September 6, 2014. https://www.economist.com/briefing/2014/09/06/too-smart-by-half; Economist staff writers, "The Pros and Cons of a SWIFT Response," *The Economist*, November 20, 2014. https://www.economist.com/international/2014/11/20/the-pros-and-cons-of-a-swift-response.
[106] TASS staff writers, "Russia to Respond to Possible Disconnection from SWIFT," *TASS*, January 27, 2015. http://tass.com/russia/773628; Gillian Tett and Jack Farchy, "Russian Banker Warns West over Swift," *Financial Times*, January 23, 2015.

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.[107]

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.[108] 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).[109] In this way, a blockchain ledger for financial transactions could make choke point strategies. That said, blockchain systems impose their own restrictions, which may make them highly unattractive.

Piecemeal worries over adversaries and resulting actions may erode global networks over the long term. More rapid change may occur if US 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 US allies, if they decided that the US was abusing weaponized interdependence in ways that conflicted with their core interests.[110] European states have been willing to accept US deployment of extraterritorial pressure, because

---

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

of "shared democratic values and indeed economic interests."[111] Currently, they benefit more than they suffer from the US exercise of network hegemony. However, this "implies that [the equilibrium of transatlantic relations] should not be disturbed by the abuse of that which certain people perceive as a form of imperialism in the domain of law."[112] Policy-makers in Europe have started to explore financing options, which are sanitized from the US financial system. While the practical effect of these specific initiatives may be limited in the short term, they put in motion a potential decoupling.[113] If the current war of words between Europe and the US over secondary sanctions devolves into fights and clashing standards, the US may find that even its allies are no longer willing to use the networks that it has weaponized to project its power.

[111] Our translation, Berger, *Rapport d'Information.*
[112] Ibid.
[113] Robin Emmott, "EU Considers Iran Central Bank Transfers to Beat US sanctions," *Reuters*, May 18 (2018).