Weaponized Interdependence

By

Henry Farrell and Abraham Newman

DRAFT – REFERENCES ARE NOT COMPLETE/BIBLIOGRAPHY TBD

Prepared for International Studies Association Conference, April 4 2018, San Francisco

Globalization has transformed the dynamics of security. In Rosa Brooks' (2016) evocative description, over the last two decades war 'became everything' thanks to interdependence. Flows of finance, information and goods across borders both create new risks for states, and new tools to alternatively exploit or mitigate those risks. The result is a world in which states are increasingly willing to employ "all measures short of war" (Wright 2017), including not just sanctions, but "lawfare" (Kittrie 2016), networks of non-state actors (Slaughter 2017) and "geonomic instruments" (Blackwill and Harris 2016) to achieve their own objectives and frustrate those of their adversaries. States' capacities to use these tools varies not only according to their internal capacities (Norris 2016), but their external circumstances.

While scholars of international relations have long considered the relationship between economic interdependence and security, their work is not well-suited to understand such dynamics, which link macro-level processes like globalization to micro-level issues of strategic advantage. Instead, existing research has tended to either focus on broad general phenomenon such as the relationship between trade and interstate conflict (Gowa 1989, Pollins 1989, Copeland 1996, Oneal, Oneal, Maoz and Russet 1996) or much more specific dynamics involving the success or failure of economic sanctions (Pape 1997, Elliott 1998, Drezner 1999, 2003, Baldwin 2000, Kirshner 2002, McGillivray and Stam 2004).

In this article, we build on an earlier tradition of work on economic statecraft (Baldwin 1985; Ikenberry 1988) to develop and apply an original argument of how external structures (specifically the network structures that arise as a by-product of economic globalization) and internal institutional capacities intersect to shape state strategic capabilities and behavior. Our argument is straightforward. Cross-national networks, contrary to liberal claims (Raustiala

2002, Slaughter 2017) 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 asymmetry. International commercial exchange – like many other complex phenomena – generates a heavily asymmetric network in which exchange becomes centralized, flowing through a few specific intermediaries. Rather than a tangled spaghetti bowl, economic interdependence produces structural relations like the 'hub and spoke' system that large airlines use to minimize transaction costs.

This means that, contrary to liberal thinking, a world of asymmetric networks is a world where power relations dominate. Asymmetric network structures create a condition of 'weaponized interdependence,' in which economic institutions and technologies devise to overcome complexity become sites of control. Some privileged states are able to leverage interdependent relations to coerce others into complying with their policy goals. Drawing on insights from social network analysis, we argue that states with political authority over the central nodes in the international networked structures through which money, goods and information travel are uniquely positioned to shape the behavior of others. Specifically, if they have appropriate institutions, which allow them to gather information or choke off economic and information flows, they can affect outcomes for other states and non-state actors, discovering and exploiting vulnerabilities, compelling policy change, or deterring actions that they do not want. We identify two specific mechanism through which states can gain powerful short term advantages from weaponizing interdependence, - the panopticon and chokepoint effects – hence achieving policy outcomes that would otherwise be impossible.

However, network structures, unlike the kinds of structure that earlier generations of international relations scholars theorized, are not entirely immutable.[1] The structures that we discuss did not arise 'in order to' become loci of power for states, or, for that matter, as a direct consequence of state action. Instead, they arose primarily because they provided commercial actors with efficiency benefits, whether through focal effects, preferential attachment, or economies of scale.

We use these theoretical concepts to develop a historical institutionalist account of how weaponized interdependence has unfolded over the last thirty years. In a first stage, the structural conditions arose which allowed interdependence to be weaponized. Here, as in more traditional structural accounts of markets and international politics, we discuss how the independent actions of many actors gave rise to unexpected structural regularities that then in turn conditioned the behavior of these actors in a self-reinforcing fashion. However, instead of perfect competition or anarchy, the structural outcome of these actors' behavior was a variety of dense, interconnected cross-national networks, in which some nodes were far more connected – and far more influential – than others.

In a second stage, privileged states such as the US and, to a much lesser extent other major states and state-like entities (China, the European Union, Russia) began to realize that under certain conditions they could exercise control over these nodes, and use them to achieve policy outcomes that would have been highly difficult to achieve in an unglobalized world.

[1] Here, we think of 'structure' from the historical institutionalist perspective of Charles Tilly and other classical 'big processes' scholars – not as an immutable external given, but as involving large scale macro-phenomena resulting from the intersecting behaviors of micro-level actors, which are *relatively* resistant over the *short-to-medium term* to efforts to change, and which may sometimes deflect even semi-successful challenges in contrary and unexpected directions.

Specifically, because these networks were cross-national in scope, and had become crucial to the proper working of national economies, privileged states were able to use their influence over key nodes in the network to shape outcomes across the various countries that the networks penetrated. The US, in particular, has increasingly looked to weaponize interdependence across a host of domains including counter-terrorism, non-proliferation, rogue states, and regime change.

We have now entered into a third 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 them in strategic terms too. Targeted states – or states who fear they will be targeted – 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.[2] 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.

This has important consequences for the interdependent relations that privileged states sought to leverage. To the extent that other states look to insulate themselves from influence, they are likely to weaken interdependence (with consequences for the efficiency benefits that

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

interdependent institutions previously produced). To the extent that these states look to poison the channels that privileged states employed and turn influence back against its source, privileged states may themselves look to gate these flows or divert them. None of this is likely to return the world to the *status quo ante* globalization, in which states maintained high borders and a great deal of autonomy. Instead, it is creating a more complex set of dynamics, in which some networked flows will continue more or less unimpeded, others will be dammed or canalized, and others still will be continually contested.

Global networks as structure

Our argument is, at its heart, structural. We contend that the various forms of cross-national economic, physical, and information exchange, which are aggregated beneath the term globalization, create patterned and relatively stable structures of interaction. These structural patterns shape the political opportunities and constraints available to states as they seek to employ coercion. Importantly, this topography is neither flat nor random but is the asymmetric product of specific patterns of market development, which forge a political geography of international exchange.

Our argument is at odds with significant scholarship on globalization, which claims that it is fragmented, complex and empowers new actors. Susan Strange (1986), as well as others who heralded the rise of private actors, have described how the international political economy diversified in the post-war period, offering business direct access to the global economy. Cerny (2010) introduced the concept of transnational pluralism, in which interest groups and

nongovernmental organizations collaborate and coordinate through decentralized channels of cooperation and communication often bypassing the state. Similarly, Slaughter (2004; 2016) emphasizes how globalization creates a more decentralized economic and political system, that generates new challenges for diplomacy. Slaughter's guiding metaphor is telling – she describes globalization as producing a network that resembles the patterns of lights that one sees from a plane during a night landing. This meshwork is a multitude of points of lights, where there are a seemingly near-infinite set of arbitrary paths that might connect any two points. These images all suggest that globalization is best understood as a set of relatively non-hierarchical relationships, in which states and non-state actors rub shoulders on a relatively equal footing.

Networks consist of two elements – the *nodes,* each representing a specific actor or location within the network, and the *ties* (sometimes called edges)*,* or connections between nodes, that channel information, resources or social influence back and forth. In simple representations, these ties are assumed to spread influence in both directions. The *degree* of a node is the number of ties that connect it to other nodes.

Standard libertarian accounts assume that networks are fluid and egalitarian – that is, that there are no major asymmetries of degree between nodes, or that where asymmetries arise they will not endure. The technical term for networks in which a new node is no more or less likely to connect to one node than another is *random graphs.* Unfortunately, the metaphor of globalization as a random graph is wildly misleading. As we discuss in other work (Farrell and Newman 2015, 2016, 2017) globalization does empower non-traditional actors, but it also gives rise to new power relations in which some actors are more equal than others. This affects relations among states, as well as non-state actors. Globalization – like other networked forms

of human activity (see Mark Newman, *passim*) – generates networks with stark inequality of influence. Hence, network structures are the consequence of the accumulated actions of a myriad of different actors, which aggregate to produce structures that bind them all. Specifically, the market focused strategies of business actors lead, inadvertently or otherwise, to highly centralized global networks of communication, exchange and physical production.

Our arguments build on the more general finding that complex systems often produce asymmetric network structures. This is one of the key conclusions of a body scholarship that is largely unexplored by international relations scholars, who, when they discuss networks, tend to focus on their consequences rather than the underlying forces that shape their topologies (Hafner-Burton, Kahler and Montgomery 2009). Such inequalities may arise in a number of plausible ways. Simple models of preferential attachment (Simon) suggest that if networks grow so that new nodes are even slightly more likely to attach to nodes that already have many ties than to nodes that have fewer such ties, then sharply unequal distributions are likely to emerge. Network effects, in which the value of a service to its users increases as a function of the number of users already using it (such as telephone networks), produce just such consequences. 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. This privileged position allows these nodes to engage in learning processes that elevate them to the cutting edge of the innovation cycle, so that others continue to link to them preferentially, maintaining and strengthening their advantage.

All of these tendencies, 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. Over the long run, these patterns can be reinforced by increasing returns (David 1990) and switching costs, in which actors remain attached to a particular standard, even when it becomes inefficient, although it is also possible that new technologies or possibilities of action emerge that substantially disrupt existing relations. The literature on large scale networks identifies many network topologies with asymmetric degree that can result from such effects. The distribution of links across nodes may approximate to a power law, or a log normal distribution, or a stretched exponential depending on particulars (Clauset, Newman and Shalizi, Clauset 2018). The statistical niceties of the distribution are often irrelevant – what *is* important is that social networks tend in general to be highly unequal in a variety of fashions.

These patterns 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. Under reasonable models of network growth, these topologies are self reinforcing – when the pattern becomes established, new nodes become overwhelmingly likely to reinforce rather than to undermine the existing unequal pattern of distribution.

Nor are these just abstract theoretical predictions. They appear to explain the observed patterns of global economic networks (Oatley, Oatley and Winecoff etc). Even when global networks largely came into being through entirely decentralized processes, they have come to display high skewedness in the distribution of degree (BARABASI, HALDANE 2009, MINOIU AND REYES 2011). More plainly put, some nodes in these networks are far better connected than others. Studies of trade (SCHIAVO, REYES AND FAGIOLO 2008, DE BENEDICTIS AND TAJOLI 2011) and banking (OATLEY ET AL. 2013, WINECOFF 2015) 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 advanced industrial democracies such as the US and (to a lesser extent) the UK (YOOK, JEONG AND BARABASI 2002).

While there is no comparable data on e-commerce, because of measurement difficulties caused by the distortions resulting from tax-efficiency seeking behavior and by lack of access proprietary data (OECD 2017), the global networked information economy is effectively dominated by a very small number of US based firms – Google, Facebook, Amazon, eBay, Microsoft and Apple. These firms prosper precisely because they benefit from the kind of asymmetric network effects discussed above, as well as economies of scale and information.

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. 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 with 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 assumed focal power – challengers not only have to demonstrate that they have a better approach, but have to coordinate the expectations of a very large number of actors away from the existing model or organization, and 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. 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 exploited similar effects to 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 that this allows, and in some cases from the unique access to information that their brokerage position provides them with.

Economic actors build and reshape these networks as they struggle to achieve efficiencies and market control. Globalization has led to the construction of new networks on a global rather than national level. Global value chains cross borders, as businesses look to disaggregate important elements of the production process. Financial relations become reconstructed in a dense web of intricate relationships across the world. Communications networks – most notably the Internet – come to span the globe.

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 globalization's development, which corresponded with US and western domination of most of the relevant innovation cycles.

In short, globalization has created a new set of structural outcomes for economic actors. Their 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. Asymmetric networks have asymmetric consequences for global power relations.

Panopticons and chokepoints

The privileged nodes or 'hubs' at the center of these networks were not typically created for the benefit of states. They variously 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, structures that were arrived at by market actors in pursuit of efficiency and market power, can be used by states for their own quite different purposes.

More succinctly, these structures are what allow some states to weaponize interdependence. States can use the interdependent structures that arose through the profit

and efficiency seeking motivations of market actors for their own strategic goals, gathering knowledge and coercing others. There are two key channels through which states can use hubs for their own purposes. The first involves the ability to glean critical and strategically valuable knowledge from information flows. This creates a public 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 myriad others. States that have physical access to or jurisdiction over hub nodes can use this influence to obtain the information passing through the hubs. Since hubs emerge as crucial intermediaries in decentralized communications structures, it becomes difficult – or even effectively impossible – for other actors to avoid these hubs while continuing to communicate BARABASI. This applies to earlier periods as well as today. Harold James notes that the ability to observe financial market activity in the City of London provided Britain with extraordinary informational advantages in the 19th Century CITE.

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 increased. The reliance of financial institutions on readily searchable archives of records converts bank branches and internet terminals into valuable sources of information. New technologies such as mobile phones become active sensors that can be tapped into by appropriate technologies. Under the panopticon effect, states' direct surveillance abilities are radically outstripped in principle 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.

The second channel, which we label the *chokepoint effect*, 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, this provides extraordinary coercive power to states that can control access to them. States or other actors that cannot access hubs can suffer very substantial consequences.

States may use a range of tools to deploy chokepoint effects. This allows us to situate existing research findings in both international political economy and international security on states' extraterritorial power. In some cases, states have direct jurisdiction over hubs, which offers them the legal authority to regulate issues of market use. A significant literature on market power, for example, highlights how states can condition market access to coerce other actors to follow its rules. A separate literature on sanctions suggests that states often blacklist certain countries from participation in certain markets as a part of the sanctions regime. The choke point effect exists on a continuum in which a state may attempt to alter the economic benefit of using the hub through financial penalties, reputational consequences, or ban access outright. The existing literatures on these various effects emphasize statecraft, credibility, the ability to involve allies and other such factors as explaining the relative success or failure of coercive policies. Our account, in contrast, highlights the crucial importance of the network structures in which all of these coercive efforts take place. Where there is one or a few hub

nodes, it becomes far easier for actors in control of these nodes to block or hamper access to the entire network.

Our account identifies two key sources of variation in states' ability to weaponize interdependence by exploiting panopticon and choke point effects. First is variation stemming from the intersection of network topology and physical geography. Only those states which have direct (or, less desirably, substantial but indirect) access to 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 and 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 China) have any real opportunity to exploit 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 the appropriate legal and regulatory institutions. Depending on domestic configurations of power and state-society relations, they may not have this, or 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. In some areas, regulatory institutions are weak or are decentralized. 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. This public policy position, which was adopted just as decentralized market efforts generated the original commercial network, make it more difficult for many European governments to exploit panopticon effects. As history demonstrates (Farrell and Newman forthcoming) domestic institutions may change in response to new perceived threats, 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.

Responses to Weaponization

The above account implies a new and different history of the last thirty years of globalization, which accentuates crucial features of interdependence that have mostly been obscured. Specifically, it suggests that globalization created new international structures governing economic, social and informational exchange across borders. These structures took the form of asymmetric networks, in which some nodes were vastly more influential than others. Although these structures were not intended to facilitate states, they turned out to provide enormous advantages to those states that (a) had access to the key relevant nodes, and (b) had the appropriate institutions to exploit them. Where these conditions were fulfilled, states – including most notably the US – consequently came to enjoy a vast informational advantage over their competitors, as well as the ability to coerce other states by denying them

access to the relevant networks. They were able successfully to weaponize interdependence to their own benefit.

This follows what scholars of historical institutionalism describe as a sequencing logic, in which changes in underlying conditions give rise to new strategies through which privileged actors can seek to use those conditions to best advantage. However, these actions can in turn lead to another round of sequencing in which they give rise to counter-reactions from other actors that perceive themselves to be disadvantaged. These actors can look to minimize their vulnerabilities in two ways. First, if they are sufficiently powerful, they may seek in the medium term to reshape constraining structures by creating their own alternative hub nodes, or even alternative networks. Here, powerful states with large markets have far more options than even relatively powerful private actors, since they can compel their firms or citizens to use new hubs and systems, partly overcoming the focal attraction of existing arrangements. Second, if they are less powerful, or are looking to achieve short term effects, they can poison the channels of interdependence to disadvantage states that have direct access to hub nodes. This is especially likely to be effective when those states face domestic institutional limits to their ability to intervene – under some circumstances it may substantially change core states' strategies.

Here, we contend that there are both tactical or short-term issues (similar to Keohane and Nye's original concept of sensitivity interdependence) as well as longer term, strategic calculations (similar to Keohane and Nye's concept of vulnerability interdependence).

We expect targets to be most susceptible to the tactical use of weaponized interdependence the more isolated they are in the network. The more that actors rely on a

single or few hubs, the more vulnerable they are likely to be the panopticon and choke point effects. The more, however, that hubs become substitutable, the greater the opportunity for targets to evade such coercion.

This obviously suggests a strategic response to weaponized interdependence. Its targets may attempt to construct or foster alternative hubs. This may be hard to do, since constructing new hubs means that states and private actors will have to forgo the economic benefits and efficiencies associated with the existing hub. One factor that plays a role in strategic resistance to weaponized interdependence concerns the relationship between state actors and private actors in target states. The greater the autonomy of internationalized private actors from the state, the less likely it will be for the state to forgo the economic benefits of the hub and subjugate efficiency gains to state security interests.

In the succeeding sections, we show how these arguments explain the sequencing of events across three core policy domains of globalization – financial messaging, dollar clearing and international data flows. In each domain, we show how a similar structural logic developed, as highly asymmetric networks emerged, in which a few hubs played a key role. 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, depending on particular domestic institutional structures. Finally, we explore how other actors have responded to the weaponizing of interdependence, by looking to change the network, to create their own network, or to turn back network effects on the US and other states that have exploited them. We conclude by exploring the likely long term consequences of the clash between states such

as the US that have weaponized interdependence, and other states looking to counter these influences.

The Rise of Network Inequality

Financial Messaging – SWIFT's Centrality

Global finance relies on a complex 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 so that they can reconcile the multitude of transactions that occur globally on any given day.

Since the 1970s, this system has been provided by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 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, which will become CITI Bank, 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 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, which is comprised of representatives from the different financial institutions involved. In an effort to sidestep the emerging rivalry between New York and London as the hubs of global banking, SWIFT's headquarters was located in Brussels, Belgium.

For much of the 1970s, it was unclear if SWIFT would be successful. The organization had to develop a new secure messaging system that could efficiently transfer tremendous amounts of data and faced a number of 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, some 11,000 financial institutions, and sharing over 6.5 billion messages annually. As Scott and Zachariadis (2014: 1) in their history of the organization conclude, "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."

Scott and Zachariadis (2014: 107) further note how an organization "founded to reduce errors and increase efficiency in interbank payments became an unexpected network phenomenon. This network effect was an accidental rather than an intended outcome. Those involved in the original SWIFT project during the 1970s were solely focused on creating an entity, a closed society, to bind members together in an organizational form that would employ standards designed to create efficiencies on transactions between the member banks."

However, despite their intentions, the organization's monopoly over financial messaging became so important commercially that it faced a competition decision 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 become dependent on the SWIFT system.

The Internet – All roads lead through Northern Virginia

Even before the Internet came into being, global data flows were heavily and asymmetrically focused on advanced industrial democracies. Controversies over cross-border

flows of data preceded the burgeoning of the Internet.[3] In the early 1970s, countries in the developing world pushed for a 'New World Communication and Information Order' that would allow states in both the North and South to better control information, leading to OECD discussions about whether "trans-border data flows" posed a problem for national sovereignty (ibid). The US government and US businesses looked to divert this debate, 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" (p. 51, Drake 2008), substituting non-binding principles for proposed wide-ranging institutions.

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. Many authorities and political actors including US President Bill Clinton believed that the Internet was 'distributed' network and effectively invulnerable to central control. In theory, no node on the Internet was significantly more important than any other, and the TCP/IP protocol underlying Internet communication was resistant both to censorship and blockages (Elmer-Dewitt 1993).

Belying its founding mythology, the underlying architecture of the Internet became increasingly centralized over time (Barabasi). Some hubs and interconnections between these hubs became far more important than others, while states increasingly were able to impose controls on traffic entering and leaving their country, while censoring or controlling many ordinary uses of the Internet. The vast majority of global Internet traffic travels across roughly 300 cables and in some areas like the interface between Europe and Africa there are fewer than

[3] Although the TCP/IP protocols that underpin the Internet were developed in the early 1970s, it received little attention outside relatively specialized academic and research communities until the beginning of the 1990s.

a half dozen cables, creating notable vulnerabilities, as do a small number of Internet exchanges, which facilitate communication across service providers and infrastructure backbones, and channel the majority of domestic Internet traffic in the United States and Europe.

Network economies 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 preferences for free flow of content across borders (except where it interfered with intellectual property), and business self-regulation.[4] US officials stymied renewed efforts to regulate the Internet through international institutions (Mueller cite), crafting a "Framework for Global Electronic Commerce" that was intended to create a global consensus for self-regulation. Domestic laws in the US provided e-commerce firms with freedom from "intermediary liability," so that they would have safe harbor (within certain limits) for sharing content that had been put up by others. This inadvertently provided the underpinnings of 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. Together with network effects, it 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

[4] Author Interview with Ira Magaziner, September 21, 2000.

algorithms rather than employees, with massive economies of scale, that quickly created very powerful incumbent firms with near monopolies such as Facebook, Google and Amazon. 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 are located in the United States. 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. One estimate, for example, suggests that 70 percent of global web traffic goes through Amazon Web Services in Northern Virginia (which had become established as a hub location earlier thanks to America Online.

Financial Markets – Dollar Dominance and the US Financial System

Globalization research often portrays international finance as dominated by footloose capital. International banks enjoy a privileged ability to exit jurisdictions that make excessive regulatory demands, leading to an inevitable race to the bottom, as states compete for the attention of business. Such accounts, however, ignore the deep structural political geography of finance and its dependence on the US dollar, US-based equity markets, and US-based financial institutions. In real life, financial firms are often only one step removed from the US market. The US's position of structural domination is complicated not by market power, but by the challenge from Europe, and the United Kingdom, which are not strong enough to topple the US, but have sufficient secondary status that they need to be taken into account.

The central position of US finance is rooted in the dollar clearing system. Since the end of World War II, more and more global transactions have come to rely on the US dollar. In some cases, this is because goods are priced in dollars (e.g. oil or sovereign debt) but in other cases it is because dollars offer a fluid mechanism of exchange. For example, Japanese or Swedish banks can both easily exchange dollar trades, while they might have more difficulty with Yen or Krona). Roughly two thirds of foreign exchange reserves held by national central banks are dollars and the next largest currency (the Euro) accounts for only twenty five percent of holdings. Eighty five percent of forex exchange trading happens in dollars and nearly forty percent of sovereign debt is issued in dollars. Moreover, US dollars dominate invoicing of global trade, with even the UK splitting its invoicing of trade equally between the dollar and the Euro. (McNamara 2008)

As the role of the US dollar has grown, more and more foreign deposits are denominated in US dollars, which are known as Eurodollars. In many cases, Eurodollars are not actual US dollars but claims among counterparties to US dollars denominated holdings held in a correspondent bank in the US. In other words, two non-US parties may engage in an exchange using Eurodollars, which then is fulfilled as their correspondent banks in the United States change dollar holdings in the United States. In order for these exchanges to happen, they have to be processed either through the Federal Reserve System or the Clearing House Interbank Payment System, known as CHIPS. CHIPS and the Federal Reserve, then, hold a privileged position in the vast majority of global transactions as they oversee transactions among US-based correspondent banks. The desire to minimize transaction costs, then, has led the

international financial system to subject payments to the direct control of US regulators, which can assert jurisdiction over dollar based transactions, even among entirely foreign parties.

At the same time, the United State equity markets and financial system play a major role not only for US firms and business but globally. The New York Stock Exchange and the NASDAQ are the first and second most important equity markets in the world, with representing over forty percent of all equities. The main rival to US equity markets is the UK, which houses both the London Stock Exchange as well as large amounts of derivatives trading. US financial institutions play a critical role internationally representing the largest block and nearly a quarter of those companies ranked as systemically important banks (G-SIBs). Once UK banks are included, the two account for roughly forty percent of the total. Importantly, for our argument, the number of such G-SIBs totals in the dozens not thousands, reflecting the broader centralization of finance. Across measures – foreign exchange reserves, market capitalization, international banking relations, OTC derivatives markets, international portfolio investment – the US (in conjunction with the UK) enjoys a central position in the global operation of finance. (FICHTNER 2016; WINECOFF 2015; OATLEY 2013). Despite a slight dip in response to the global financial crisis, the US position has since stabilized or increased.

Weaponizing the Hubs

SWIFT, Counter-Terrorism and Non-Proliferation

SWIFT illustrates how large states such as the US have been able to exploit both the panopticon and choke point effects. Precisely because SWIFT had become such a central hub in

the international payment system, recording the vast majority of global financial transactions, it came to be strategically valuable. States – most importantly the US – came to consider how they might use information on for surveillance and leverage the financial sector's dependence on SWIFT as a tool of asymmetric influence.

Although many observers focus on the attacks of September 11th 2001 as the moment when governments began to consider SWIFT's value for surveillance, they had begun thinking about SWIFT's potential much earlier. 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. 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."[5] In response, SWIFT argued 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 information requests.

While the organization was able to keep governments at bay for much of the 1990s, the attacks of September 11 created a greater sense of urgency among governments, and a greater willingness among SWIFT officials to accede to their demands. In the wake of the attacks, the

[5] Quoted in Scott and Zachariadis (2014: 128)

United States government led by the US Treasury began to examine ways to use the global financial system to curtail terrorist financing, targeting the terrorist money supply. This Treasury initiative became known as the Terrorist Finance Tracking Program (TFTP). Treasury's initiative to press SWIFT into service was a key component of this effort. After an initial rebuke by SWIFT, the Treasury obtained legally enforceable subpoenas to gain access to SWIFT records. It was hard for SWIFT to resist the Treasury's demands because the organization had a US based mirror data center in Virginia, which fell under US jurisdiction. In the years that followed, SWIFT secretly served as a global monitor for US anti-terrorism efforts, with the Treasury department able to use the SWIFT system to monitor and investigate illicit activity. As Juan Zarate, a former treasury department official explained (2013: 50), "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." Treasury officials argued that TFTP was a central tool in the global war against terrorism. When the existence of the program was revealed by *New York Times* journalists, leading to uproar in Europe, US officials including Hillary Clinton, then Secretary of State, and President Barack Obama were involved in an extensive effort to defend the program.

Efforts to weaponize SWIFT, however, were not limited to the panopticon effect. Policy-makers used the SWIFT system more openly, in order to enhance sanctions against the Iranian regime. Beginning 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 Iran. The group targeted SWIFT as complicit in assisting

the Iranian regime and contributing to its economic health. As SWIFT's 2010 annual report noted, some 19 Iranian banks as well as another 25 institutions relied on the messaging system. 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." The campaign was quickly taken up by policy-makers in 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. The European Union followed up on US threats in March, passing regulations that prohibited financial messaging services (e.g. SWIFT) from providing services to identified sanctions institutions. As Lazaro Campos, former CEO of SWIFT, concluded, "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."[6] The Iranian regime quickly felt the consequences of the SWIFT noose tighten as its major financial institutions, including its central bank, found themselves locked out from the international payment system, creating large scale economic disruption.

The NSA, PRISM and Counter-terrorism

The US enjoyed similar – and arguably even greater – dominance over information networks and e-commerce firms. However, it was far less eager to deploy the chokepoint

[6] SWIFT press release, March 15 2012.

effect, both because of domestic institutional constraints, and a belief that the US would benefit from the global diffusion of communication technology and dominance of US e-commerce firms. The US commitment to self-regulation of e-commerce meant that it had relatively few means to oblige technology companies to do its bidding, and even where it did have such means, it faced 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.[7]

The US, under the Clinton, Bush II and Obama administrations, believed that open communications helped spread democratic values, and was thus strategically and normatively beneficial for the US. In a much remarked upon major speech, Secretary of State 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."[8] The US sought 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.[9] The action was controversial, and was not publicly repeated.

---

[7] See Daniel Kehl, "US Government Clarifies Tech Authorizations under Iranian Sanctions," *New America*, February 14, 2014.
[8] Hillary Rodham Clinton, Remarks on Internet Freedom, January 21, 2010.
[9] Mark Landler and Brian Stelter, "Washington Taps into a Potent New Force," *The New York Times,* June 16, 2009, available at

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."[10] US officials looked to protect the Internet from a variety of non-US efforts to bring the Internet under the control of multilateral organizations (Segal 2017).

Even while the US abjured chokepoints and promoted the cause of an open Internet, it began to take quiet advantage of 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. In the blunt description of former NSA Director Michael Hayden:[11]

> 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?

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

---

http://www.nytimes.com/2009/06/17/world/middleeast/17media.html?_r=1&scp=2&sq=Twitter&st=cse.

[10] 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.

[11] 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/.

simultaneously worried about being seen as "instruments of government" but willing to recognize that they needed to cooperate with the government on key issues (ibid). 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 has demanded the cooperation of telecommunications companies in carrying out "upstream collection" of large amounts of data from the Internet backbone. This effectively allows the US to copy this data in bulk, and then later filter it for valuable information, while complying with US laws that distinguish between the data of US and non-US citizens ('incidental collection' of data on US citizens is permissible). The US gathered data *inter alia* from switching stations, 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.

After 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 (Farrell and Newman, forthcoming). However, as best as can be discerned the US model of surveillance based on its privileged access to network nodes was left relatively unaffected by these changes.

Secondary Sanctions Against Rogue Actors

The reliance of foreign actors on the dollar clearing system and US banks and equity markets has provided the US with leverage in areas as diverse as foreign bribery, anti-trust and insider trading, US regulators have leveraged the nexus between US financial institutions and US jurisdiction, obliging compliance with US law and often ambiguous regulatory guidance.[12] In particular, after September 11 2001, the US government and the US Treasury, however, sought to use this nexus to bolster national security, by denying 'rogue actors' access to the main flows of the international financial system, pressing foreign banks into the service as effective agents of US policy through the chokepoint and panopticon effects.

The basic logic behind the US strategy was to use third party financial institutions go after the money which kept terrorist groups and rogue states economically viable. Juan Zarate (2013:10), assistant secretary for terrorism financing and financial crimes under the Bush administration, explains "the most important insight powering Treasury's campaign was its focus on the financial sector's omnipresence in the international economic system…The banks are the ligaments of the international system. In Treasury, we realized that private-sector actors – most importantly, the banks – could drive the isolation of rogue entities more effectively than governments – based principally on their own interests and desires to avoid unnecessary business and reputational risk." The Treasury strategy was viable because these global firms

[12] Loeffler, former deputy director of global affairs at the US Treasury Department, 2009. "U.S. national security policy and the international banking system have become inextricably intertwined."

depended on US dollar clearing, equity markets, and financial institutions. Upending these relationships would put targeted firms under tremendous financial strain.

This strategy was rooted Executive Order 13224 and Section 311 of the Patriot Act. Executive Order 13224 allows the Treasury to freeze the assets of terrorist individuals or entities as well as organizations and businesses that *provide support to them*. In President Bush's words, "We're putting banks and financial institutions around the world on notice – we will work with their governments, ask them to freeze or block terrorists' ability to access funds in foreign accounts…If you do business with terrorists, if you support or sponsor them, you will not do business with the United States of America." The Executive Order was complemented by a relatively obscure section of the Patriot Act (section 311), which allows the Treasury to designate jurisdictions, institutions, or classes of transactions as 'primary money laundering' concerns. Once an entity is deemed a primary money laundering concern, third parties that interact with that entity risk running afoul of US law. In the words of Zarate (2013: 152), "The intent of this strategy was to drive the private sector's isolation of these banks, placing the onus on the banks to police their own system. It would also place added pressure on the criminals and rogue regimes that were relying on those banks to do business globally".

This strategy relied both on the panopticon and chokepoint effects. Treasury used the threats of engaging the executive order 13224 or Patriot Act Section 311 process to obtain information from foreign financial institutions and to cut rogue actors off from financial networks. Treasury exploited the financial traces left as these actors engaged in their day to day business. In the description of Treasury Department's general counsel, David Aufhauser, "books and records that are not intended for public oversight do not lie; they are literally the diaries of

the enterprise of terror."[13] At the same time, the Treasury exploited the centrality of the US financial system to threaten the financial operations of cooperative institutions. Here David Cohen, Treasury's Under Secretary for Terrorism and Financial Intelligence, details how such chokepoints operate:

> For banks and businesses around the world, if they don't have access to the US financial system, don't have access to the US economy, it is a significant if not mortal wound. That gives us a huge amount of leverage, a huge amount of opportunity to project US power through our financial institutions.[14]

This leverage does not simply reflect the vague reach of US hegemony but instead corresponds to the political geography of finance. As one journalist familiar with the process used by Treasury explains, "OFAC's targeters comb through classified intelligence reports, financial records and corporate registrations. They build charts illustrating how striking one financial node will impact other nodes…"[15] The reach of such leverage is amplified by the ripple effects of reputational and compliance risk. Once US financial institutions raise another firm's risk-level, global financial institutions fear that there might be credibility contagion. Moreover, companies fear getting entangled in US enforcement actions. One US law firm explains,

> Because these [rules] at times seem almost purposefully confusing, many non-US financial institutions are carefully scrutinizing business because of the mere possibility, however remote, that an attenuated Iranian interest in a transaction would expose the

[13] An Assessment of the Tools Needed to Fight the Financing of Terrorism: Hearing Before the S. Comm on the Judiciary, 107th Congress (2002): 17

[14] William Mauldin, 2014, "US Treasury's Top Terrorism Cop: How Financial Tools Fight Foes," Wall Street Journal, June 2.

[15] Anna Yukhananov, 2014. "After Success on Iran, US Treasury's Sanctions Team Faces New Challenges," Reuters April 14.

> bank to sanctions, possibly to a significant fine, and to adverse publicity. The strongest impact of these sanctions may be their mere existence rather than their exercise, as highly-regulated and risk-averse financial institutions steer well clear of the line.[16]

As Juan Zarate further explains how starting a Section 311 process leverages the network-based system to the US advantage against a foreign financial institution, "make them radioactive to reputation-conscious banks worldwide."[17]

The Treasury, then, weaponized the global reliance on the US financial system against the Al Qaeda terrorist network and then a series of adversarial states including Syria, North Korea and Iran. In September 2005, for example, the Treasury used Section 311 to designate the Banco Delta Asia (BDA), a small private bank located in Macau, as a primary money laundering concern. The bank, which was quickly isolated from the international banking system, had 'tailored its services to the DPRK [Democratic People's Republic of Korea]'s demands…Banco Delta Asia's special relationship with the DPRK has facilitated the criminal activities of North Korean government agencies and front companies.'[18] The 311 action, however, did not just eliminate this one middleman of the DPRK, but quickly led other central financial institutions to apply additional scrutiny to and freeze accounts, which might be suspected of having links to North Korea. In other words, the hubs began to worry that they too might be implicated. The effect of the action is captured by Victor Cha, a North Korea expert and former Trump nominee to become Ambassador to South Korea, "It was a smash in the

[16] Colin Simpson, 2013, UAE Business to Feel Effect of Fresh US Sanctions on Iran. National, July 3.
[17] Zarate, page 152. Cite Feaver and Lorber here
[18] Quoted in Zarate page 240.

mouth, a slap in the face. When they first heard about the action, they just thought it was another sanction, but four weeks later they realized what had hit them. It really got the North Koreans to sit up and notice that this was a tool they'd never seen before, and frankly, it scared the shit out of them."[19]

The US government turned to similar tools as it sought to shift the terms of debate in their negotiation with Iran over its nuclear program. In 2006, for example, the Treasury limited the ability of US banks to perform dollar clearing for specific Iranian banks. This included Bank Saderat, one of Iran's largest state-owned banks. Ending the ability of Bank Saderat to use the US dollar clearing system made it hard to clear oil transactions (priced in dollars) with other foreign banks. Then in 2010, Congress further deployed the financial chokepoint through the Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA). As in the case of North Korea, the act targets foreign banks conducting business with Iran, who participate in U.S. financial markets. The Treasury is empowered to limit the access of these foreign banks to US markets. Again, the threat of such an action carries potentially significant reputational damage. The US government escalated pressure in 2012 when it placed additional restrictions on US and foreign banks offering correspondent banking services to Iranian financial and energy companies. Equally important, the Treasury singled out a number of important international banks (ING, HSBC, BNP all faced with multimillion dollar settlements) and prosecuted them for failing to comply with U.S. secondary sanctions. While the exact impact of these efforts on Iran is hard to discern from public sources, numerous anecdotal accounts attest to the ways in which these chokepoints altered the Iranian negotiating position over its nuclear program.

[19] Quoted in Zarate, page 245.

Different administrations have made clear how important they believe these tools to be. Treasury Secretary Hank Paulson warned "This is one of the most powerful actions that can be taken, short of military action,".[20] Similarly, the New York Times described the Treasury as "Obama's favorite noncombatant command."[21]

Resisting, Join or Submit

As the above narratives suggest, many other states did not initially understand how asymmetries in globalized networks allowed the US (and to some degree the EU) to weaponize the hubs. Once the US began to properly exploit them, others, particularly powerful states such as China and Russia, quickly had to address the threat and consider a response. The network effects, which underlie the hubs' prominence, has made it hard for states that depend on their business community and on global markets to resist these effects. Other states have attempted to coopt the power of the hub, trying to bandwagon on the panopticon or choke point effects. For example, the European Union, which initially resisted US efforts to weaponized SWIFT, ended up by cooperating in exchange for access to information, and is now considering changes that would extend TFTP style surveillance to other financial transactions. A final group, by contrast, including most prominently China and Russia, has looked to resist US network dominance, routing around its control functions.

<u>Reciprocity versus Blockchains</u>

[20] Robin Wright, 2008, "Stuart Levey's War," The New York Times October 31.
[21] David Sanger, "Obama Policy is Put to Test", New York Times, March 17, 2014, A1.

When, in 2006, the New York Times reported on US-SWIFT cooperation, revealing the program to the world, European civil liberties advocates called for the program to be shut down. They argued that it was inconsistent with domestic privacy rules and as SWIFT was headquartered in Europe, European privacy rules should apply. This put SWIFT in a delicate position as it faced a policy double bind – breach US security requirements or EU privacy rules. At the same time, security-oriented groups in Europe saw much to like in the TFTP program as it opened up access to a critical information hub, which had long been kept dark by domestic privacy rules.

Europe's response illustrates both the resilience of hubs and the temptation, where possible to bandwagon on the panopticon effect. On the one hand, SWIFT attempted to quarantine European data by creating two zones for its data storage. One, located in the EU maintained files on EU transactions. Another, kept in the US, managed global interactions. At the same time, however, the US and the EU negotiated an agreement, the SWIFT Agreement, which detailed a set of procedural rules allowing them to share data for security purposes. These offered some privacy protection for the messaging system. But equally important, the Agreement contained a reciprocity clause, in which European security officials could ask US Treasury to access the TFTP program on their behalf. In this way, European security officials could have their cake and eat it too, arguing that they maintained European privacy rules, while also accessing information gathered via the panopticon effect.

Russia, in contrast, has sought to secure itself against efforts to weaponized SWIFT. In the immediate wake of the US-Europe response to its invasion of part of Ukraine, XXXX stated that XXXXX, implying that any efforts to restrict Russian access to SWIFT would result in an

extremely serious, and possibly even military response. Russia has since sought to build up an alternative system that would limit its own vulnerabilities both to surveillance and denial of access. Specifically, in the recent past, Russia has begun to explore the promotion of blockchain technology, popularized by BitCoin. The advantage to such systems is that they rely on a decentralized accounting system. Rather than a central node, which processes all messages, each member of the network has its own directory of transactions. As a result, blockchain infrastructures undercut control efforts that target a central hub. They are more resistant to monitoring than traditional financial transfers, although they scale poorly, and are not nearly as resistant as some of their users believe (it is often possible to painstakingly reconstruct financial flows from the evidence of the blockchain). At the same time, states like Russia will face their own challenges in regulating and monitoring these new payment systems. While blockchain may evade the watchful eye of the US Treasury, it will also obscure similar efforts by the Russian federation. INTRODUCE NEW EVIDENCE

China has followed a third strategy, developing its own parallel messaging system (Cross-Border Interbank Payment System CIPS) operated by the Bank of China.[22] First proposed in early 2012, as US secondary sanctions mounted, it became fully operational in October of 2015. CIPS is not yet ready to replace SWIFT. It has far fewer members and is focused narrowly on facilitating transactions between corresponding banks, rather than a full scale messaging system. That said, it already has X members. In 2016, it signed a Memorandum of

[22] Gabriel Wildau, 2015. "China Launch of Renminbi Payment System Reflects SWIFT Spying Concerns, Financial Times, October 8; TASS. 2015. "Russia may use China's Payment Infrastructure instead of SWIFT – VTB Bank Head." March 11.

Understanding with SWIFT, allowing for interaction across the platforms.[23] Nevertheless, the Chinese government sees CIPS as a key tool to undergird the expansion of international transactions in yuan. As one observer noted, "CIPS will also begin by using SWIFT for interbank messaging, but eventually the system will have the ability to operate independently. In the future, CIPS will move in the direction of using its own dedicated communications line. At that point, it can completely replace SWIFT."[24] Ultimately, the CIPS effort could undermine the ability of the US and EU to deploy the chokepoint and panopticon effects against Chinese financial institutions, and possibly other countries' financial institutions that joined the CIPS system.[25]

Data Localization

Non-democratic countries had begun to insulate themselves from the "open Internet" long before the Snowden revelations. Most notably, China had created an extensive set of controls designed to forestall open mobilization against the ruling party. The "Great Firewall of China" has multiple interconnected components, which are designed to prevent Chinese citizens from gaining access to specific websites located overseas, or viewing content containing specific words. These go together with an extensive domestic censorship and surveillance regime. Research on this regime suggests that the Chinese government's primary concern is counter-mobilization – while it is prepared to tolerate certain kinds of criticism

[23] SWIFT. 2016. *SWIFT and CIPS Sign Memorandum of Understanding on Cross-Border Interbank Payment System Cooperation*, March 25.
[24] Wildau. 2015.
[25] See Rotblat. Footnotes 183. See also, Lloyd Gumbo. 2015. "CIPS: Liberating World From US Financial Tyranny," Herald, October 14. (Zimbabwa newspaper)

(albeit with variation, and a tendency to crack down during particularly sensitive periods), it is not willing to allow communications that might actively mobilize citizens (King, Pan and Roberts 2013). China has also successfully prevented US social media and search companies from establishing a significant foothold in Chinese territory, instead fostering domestic companies such as Alibaba and WeChat, which have clearly established themselves as alternatives to US-based platforms in a way that European companies have not. Other authoritarian countries, such as Saudi Arabia, Iran and Egypt have also introduced censorship measures against Internet communications. Some, such as Egypt, have increasingly turned to Facebook as a possible source of information about the social networks of dissidents.

Russia, in contrast to China, has not established an effective general censorship regime. However, it has come to see open Internet communication as a threat to the Russian government's domination, especially in the aftermath of the "Color Revolutions," the "Arab Spring," and the overthrow of a Ukrainian government friendly to Moscow and its replacement with a pro-Western regime. It has looked to ensure that domestic media are owned by 'friendly' oligarchs, and like China has also relied on "flooding" attacks to hamper counter-organization (Tucker et al. 2017, Roberts 2018). Such attacks involve destabilizing online political conversation through a combination of automated bots and trolling, less intended to change people's minds than to produce sufficient distraction, confusion and despair as to make it impossible to talk, let alone organize online.

European states, in contrast, have continued to support an open Internet. However, they have taken steps in response to the revelations of US use of the panopticon effect. The "Safe Harbor" arrangement through which US companies could bring the personal data of

European citizens back to the US was declared *ultra vires* by the EU's Court of Justice, which has taken an increasingly activist role in policing international data transfer arrangements. Its successor agreement, the so-called Privacy Shield, is also in substantial legal jeopardy. US e-commerce companies, fearing reputational damage, are now far less likely to cooperate with the US, except when absolutely legally necessary, and have begun to fight the US government in court. Notably, companies such as Google have both systematically begin to encrypt their own data transfers so as to prevent easy 'upstream' collection and are taking steps to provide other Internet content providers with the incentives to encrypt their own transfers too. While this will not completely undermine the US ability to use its panopticon, it will (barring some grave unknown flaw in the standard encryption protocols) make it much more cumbersome.

Perhaps the most unexpected change has been the increased willingness of Russia to use Internet openness against the US government. After deploying flooding attacks against its own opposition voices, Russia has begun experimenting with using them as an external strategic weapon. In the 2016 presidential election, Russians not only hacked sensitive political servers, but also used social media to carry out a variety of attacks intended to heighten social, political and cultural attacks in the US. These attacks were often inept, but nonetheless effective, not least in greatly increasing the general paranoia of US citizens about manipulation.

This presents the US with a series of awkward choices. Taking strong action against these attacks will require major changes in the practices of US social media companies, such as engaging in much more individual and specific monitoring of their users and commercial customers. These firms are likely to be unwilling to take such action, because of the grave risk it would pose to their business model, forcing the US to decide between accepting such attacks or

changing its fundamental commitment to self-regulation on the Internet by imposing detailed and intrusive mandates.

Furthermore, preventing such attacks might water down the US commitment to open communications, because many such attacks by their nature will be nearly indistinguishable from more ordinary political communications and attempts to persuade. While Russia and China would likely be willing to negotiate a broad document guaranteeing non-interference using digital means in domestic politics, they would demand that the US in turn recognize their own rights to non-interference, undermining the US international commitment to online freedom.

Replacing the Dollar System? Rogue State Cooperatives or New Reserve Currencies

As the US government has leveraged the centrality of its financial system, there is a clear risk that other powerful states will attempt to reduce their dependence on dollar clearing, US financial markets and financial institutions. These state-led efforts, however, face an inevitable backlash from market actors from these countries, who are reluctant to forgo the economic efficiencies of the current network structure. Here, the relationship between states and their business elites will likely play an important role in the extent to which the state can evade the panopticon or chokepoint effects.

Policy-makers across the world recognize the potential threat to the US-based system. As former Secretary of the Treasury Jacob Lew explains, “We must be conscious of the risk that overuse of sanctions could undermine our leadership position within the global economy, and the effectiveness of the sanctions themselves…financial transactions may begin to move

outside of the United States entirely, which could threaten the central role of the U.S. financial system globally, not to mention the effectiveness of our sanctions in the future."[26]

At this point, China and the Yuan seem to be the largest beneficiary of such defections. Chinese academics and think tanks have actively pressed for the Chinese government to exploit the opening. In a recent book, Ma Xin (2013) argues, "As America increasingly utilizes financial sanctions and its financial power, it also increasingly encourages peripheral countries to 'de-dollarize.' This gives the internationalization of the yuan a strategic opening."[27] As a proof of concept, Iran and Russia have begun to clear commodities trades in Yuan instead of US dollars.

The ultimate consequence of these interactions, however, is far from clear. Many of the markets such as China, which might hope to develop an alternative reserve currency, face significant internationalization barriers. At the same time, potential clients, such as Russian firms, still rely on foreign banks in Europe for much of their transactions and these European banks, in turn, have significant exposures to US financial institutions. Here, the transitive property of network relations significantly mitigates resistance strategies.

Conclusion

In this article, we have laid out a case for reconsidering the relationship between interdependence and coercive state power. As we have shown across three key areas, globalization has led, to a massive increase in cross national exchange and cross national networks through which economic actors have looked to achieve efficiency gains. However,

[26] Jacke Calmes. 2016. "Lew defends Sanctions but Cautions on Overuse," New York Times March 29

[27] Quoted in Rotblat 2017: 312.

these networks were not symmetric but heavily asymmetric, so that some nodes were far more important than others. The consequence has been threefold. First, that it has been possible to weaponize interdependence – that is, to use the cross-national networks and relationships that interdependence has resulted in – in order to achieve effects that would otherwise have been costly, difficult, or perhaps even effectively impossible. Second, that some states have been far better placed to weaponize interdependence than others. Specifically, states that have control over key nodes have been able to achieve strategic benefits and shape outcomes through exploiting the panopticon and chokehold effects. Finally, that as these states (most prominently the US) have taken increased advantage of those possibilities, other powerful states have looked to defend themselves through withdrawing from the relevant networks, subverting them, or creating their own.

These findings have important implications for existing debates. First, and most obviously, they provide a compelling alternative to liberal accounts of globalization and international networks. Liberals have systematically treated such networks as decentralized opportunity structures that facilitate general cooperation among both states and non-state actors. They have not received much pushback on these claims, because realists have not typically concerned themselves with the politics of interdependence, which seems both removed from the realm of security, and bound up with a set of theoretical claims about the willingness of states to depend on others that they tend to find unconvincing. Like realists, we start from a set of assumptions about the primacy of power in international relations – but we root our understanding of power relations in a very different set of international structures (and in a differing understanding of structures) than realists do. This reveals a deep irony in

liberal accounts, as economic institutions, which were created to promote efficient market interactions, have become powerful sites of political control. It also allows us to precisely identify the systematic ways in which existing liberal accounts underplay the power politics of interdependence, and to provide an alternative understanding, rooted both in network theory and historical institutionalism, through which we can explain key aspects of global politics that often go unremarked in current debates.

Our arguments furthermore provide a new way of understanding the renascent literature on statecraft. Both policy scholars (Brooks, Wright, Blackwell) and academics () have looked to understand the ways in which the US and other states use non-traditional forms of power in order to achieve their ends. However, their accounts tend either to focus on the specific conjunctural circumstances that face US policy makers, or to explain the capacity of states to engage in statecraft by looking to their domestic capacities. Our account, in contrast, brings together both domestic capacities and international structures into a common explanatory framework, examining how they interact to provide states with greater or lesser opportunities to exploit interdependence for their own ends.

Finally, we believe that our framework will help other scholars and writers to identify commonalities across problem areas that are usually not considered together, as well as identifying important new questions. Some areas of weaponized interdependence – such as sanctions – have been the subject of extensive research. However, next to none of this research has focused on the interaction between global structure and domestic capacity that we consider to be crucial to explaining outcomes, and sanctions have largely been treated on their own, rather than compared to other areas of economic and security statecraft. Our framework

allows us to do both. It also allows us to begin thinking about a host of new and emerging security questions. Over the last eighteen months, it has become clear that communications networks can have general security consequences that go far beyond the kinds of effects explored by cybersecurity scholars, who tend to draw their analogies and understandings of international politics from traditional security, with its focus on expectations, offense versus defense dominance and the possibilities of deterrence. If we are to understand properly, for example, the ways in which communications networks can be turned against democracies, we need new frameworks that are better calibrated to capture the politics and their effects. More broadly, these examples demonstrate the limits of current divisions in the field, which delimit security and economic issues, and instead calls for an integrated approach, which examines the fundamental ways that they are intertwined with each other. The framework of weaponized interdependence that we offer provides one fruitful way to begin doing this.