Key Trends across a Maturing Cyberspace affecting U.S. and China Future Influences in a Rising deeply Cybered, Conflictual, and Post-Western World

Dr. Chris C. Demchak

Testimony before Hearing on China's Information Controls, Global Media Influence, and Cyber Warfare Strategy

Panel 3: Beijing's Views on Norms in Cyberspace and China's Cyber Warfare Strategy

U.S.-China Economic and Security Review Commission

Washington, DC

4 May 2017

The views expressed here are those of the author alone. They do not represent the views of the U.S. Navy or any other organization of the U.S. government.

Over the coming century, consolidated[1] democratic civil societies will be a numerical minority in a deeply cybered and conflictual world dominated by non-western autocratic states.[2] Now well into its rise as the center of economic and demographic power in the emerging post-western world, China has the advantage of an enormous scale in market and resources, as well as a rising momentum internationally as an alternative model and large new ally for existing and rising authoritarian leaders globally. Since the bulk of the world tends toward authoritarian political cultures and structures, China will by all measures be particularly able to channel – if not dictate - the rules in practice across the international system using its deeply embedded regional, economic, and cybered bonds.

While this rise of the 'rest of the world' (ROW) was inevitable, westernized democracies have lost their leadership role in the international system faster and more pervasively than might otherwise have occurred if there had been no – or a different form of – cyberspace. Today's cyberspace is a global societal 'substrate', not a 'commons' or an administratively convenient 'domain'. As such, it critically connects societally essential functions domestically and globally. However, it was built on insecurely coded foundational architectures, widespread utopian misperceptions of the internet, a libertarian corporate commercial fixation that prioritized market access over national or systemic security, and an overarching complacency across western states about the inevitable domination of their vision of democratic civil society and international rule of law. In reality, cyberspace has accelerated intra – and inter-state massive economic exploitation, and reinforced the wealth extraction and societal control of personalized political control across the non-westernized majority of the globe.

[1] The term 'consolidated' is used to distinguish a stable, functioning, modernized, democratic civil society from a developing nation recently civilianized, highly corrupt, prone to military coups, or ruled by a single party or strongman, yet which occasionally has what are generously called open elections and thus is labeled a democracy. (Diamond, 1994)

[2] Much of this discussion draws upon a previous 2016 publication. See (Demchak, 2016)

The shoddily built cyberspace, in particular, created and spread a new form of system-vs-system 'cybered conflict"[3] China's scale and its ever growing skill in this form of conflict challenge democratic societies' influence over the interstate system and would do so in any case. However, the democratic civil societies have themselves equally to blame for much of the cyber threats emergent today due to their own blinders and failure to act early and collectively. Today, western states experience between 1 to 2 percent annual GDP loss due to cyber insecurity affecting societal rules, economic resources, and national security capabilities. (PWC, 2014) (Hathaway, 2013) This "greatest transfer of wealth in human history" constitutes the hollowing of the future assets needed for the long-term, agile and effective defense of democratic states. (Paganini, 2013)

This testimony will argue four points about the sources of – and solutions to – these trends now threatening a tsunami of offense and extractive campaigns, to which open democratic civil societies remain especially vulnerable.

I. Summary Points

1. The internet grew up too fast, too cheap, and too shoddy, and now must be transformed with security as equally embedded as freedom speech is assured, and generativity is encouraged. Western utopianism and libertarian IT capital goods industry security-blindness laid the foundation for today's unprecedented system-vs-system "cybered conflict" by changing five fundamental constraints on offensive campaigns in modern conflict: scale, proximity, precision, deception in tools, and opaqueness in origins. Cybered conflict then blended with the routine systemic surprises routine found in all largescale complex systems to jointly impose four layers of complex system surprise unique to the cybered era (single firm, critical infrastructure, huge bad actor community, and small deeply skilled advanced threat groups). With such a poorly secured substrate, a modern state is now a deeply interdependent huge socio-technical-economic system (STES) whose economic vitality and societal stability are exquisitely vulnerable to predators and adversarial states. Only transformation of the underlying architecture will change the dynamics to something more manageable and less hollowing for democratic civil societies.

2. Borders are rising in cyberspace across authoritarian and democratic states, and this trend must be accommodated, rather than resisted by democratic states. While China has adamantly maintained a right to its cyber sovereignty, it has also massively exploited the open borders of wealthier western societies, bringing the intellectual property (IP) advantages in technologies to market and future wealth inside its own more controlled systems. In the face of this reality, western states are domestically installing defenses and controls while denying this reality in public policies and international statements. Western libertarian IT capital goods industry leaders are loudly arguing for zero regulation of their activities in democracies while quietly complying with the technology transfer, privacy denying, or other demands of authoritarian government

[3] 'Cybered conflict' is a term adopted to indicate the conflict is systemic and so likely to be deeply integrated into conflict in the future that the term 'cyber' should eventually be discarded as redundant. For the moment, however, it is necessary to retain the adjective to keep the fundamental trend in view and in discussion. For its first use and explanation, see (Demchak, 2010)

elsewhere. Our western refusal to recognize rising national jurisdictions in cyberspace for our peculiar utopian and libertarian economic reasons appears hypocritical and has more rapidly reduced the influence of western civil society values. In being so distracted by this losing battle, we encouraged the rise of a Chinese narrative as an alternative story path combining economic success and domestic internet control. We also ignored our own urgent need for a collective resilience narrative – a cyber economic 'stateness' story. Without it, we are unable to coalesce public and private efforts aimed at the protection of our openness and economic vitality in a cybered age. In the interim, the rise of a Cyber Westphalia is changing the topology of the international economic system to reflect more authoritarian internet preferences.

3. The demographic scale is the major Achilles heel of the consolidated democratic societies in a deeply connected world facing a single coherent and cyber aggressive actor the size of China. Only by presenting a competing, competent, and size equivalent alternate cyber power can these states defend their collective cyberspace and future wellbeing. For China's leaders, this scale is their main argument for their "rightful place' in the world. Consolidated democratic societies are a minority community - relatively few (perhaps 40 at best in a world of 196 countries) and small to medium in average size. As trends stand, China's economic weight, rules demands on smaller partners, and sheer presence will majorly define the preferences of the emerging, highly connected, post-western world. As trends stand today with no coherent counterbalancing democratic weight, the international system will increasingly reflect Chinese business and organizational memes: low transparency, hierarchy of big over smaller, self-censored communication, and highly personalized business practices. (Tan & Tan, 2012) That situation will be reinforced with the rise of a more authoritarian rest of the world connected by Chinese technologies and paid for, run, maintained, operated, and updated by Chinese firms, especially in telecommunications. Western civil societies operating independently in their own cyber defense of their vulnerable STESs will individually eventually have to concede to the dominant practices of this emerging nonwestern world. Only by creating a coherent functionally integrated and operationally systemic 'cyber resilience alliance' will the minority community of consolidated democracies be able to extract restraint and peer power accommodation on the part of China and the larger number of its fellow authoritarian states. Otherwise, the exchange preferences requiring transparency and impersonal relations of the liberal economic international system will be reduced to mere formalities, if that.

4. Such an alliance is feasible because a community of at least 900 million citizens will have the economic market weight and the technological talent pool to face China as a peer in a conflictual cybered world. Such a unified systemic cyber resilience alliance can orchestrate its own shared adaptive sensor and mitigation systems, massive R&D programs to both universities and firms, and the economic and technological talent to transform the collective cyberspace. [4] The shoddy substrate can be reformulated to be fundamentally secure, fair, open to global trade, but not so easily remotely exploited for economic advantage and cybered conflict.[5] Such a collectively integrated, coherent 'actor' can provide the framework and urgency to build the necessary civil society

[4] John Mallery of MIT has spoken wide and long on the need for this fundamental transformation as the only real long term survival path open to consolidated democratic civil societies. (Mallery, 2011 (2009))

[5] A number of authors have more recently been speaking out on the need for this kind of 'like-minded' alliance, but few have gone further to give it structure and, importantly, a mission distinct from saving the entire world's internet as this piece argues. For recent works that move in the direction of needing such an alliance, , see (Nye, 2014) and especially the latter chapters of (Segal, 2016).

stateness needed. Its structure and mission to maintain a unified all sector response actively engages the private IT capital goods sector in the defense of the democratic economic system as team players, citizens, and still globally vigorous competitors. The inclusive responsibility for defense and generativity of all sectors across the alliance is critical. The scale of the authoritarian rise and their national jurisdictions will dismantle the civil society values embedded in the currently liberal international economic system, leaving only remnants of the open internet along with the fair market rules of today. China already speaks of eventually displacing the shoddily built westernized technologies with those said to be less exploitable and destabilizing, including for security pervasive surveillance and content and access controls. Chinese technology companies are globally routinely now in the top three ranks across a host of critical components of the cyberspace substrate. When their preferences in design and production dominate cyber-related markets globally, democratic societies will individually not have the means to secure their own cyber substrate supporting democracy and the transparent, free exchange of accurate, unmanipulated information over the long term. Only with such an alliance can democratic societies afford the necessary large push combining in talent and investment to keep healthy markets with alternative technologies able to transform the basic internet technology at the proper scale to defend the economic well-being of their nations in the future. With these nations capable of acting in unity, they will be to no small extent more cyber autarkic and resilient. In so doing, the consolidated democratic world will create the robust cyber power jointly needed to negotiate with the rising authoritarian world – and China – for equitable rules and acceptable societal wellbeing in the emerging highly conflictual cybered age.

II. Built Poorly on Utopianism, Security-Blind IT Capital Goods Libertarianism, and Hubris[6]

Cyberspace is widely misunderstood and has been from its outset. It is now a deeply intertwined ‘substrate’ connecting all the critical components of every nation’s domestic ‘socio-technical-economic system’ (STES), built with fault-tolerant programming and insecure hardware routinely sent too quickly to market with overblown promises of fast returns. Three interrelated cognitive blinders in western approaches to the spread of cyberspace hindered accurate assessments of the emerging reality. These were unrealistic optimism in early utopian cyber visions blended with security-blind IT capital goods business models, and endured far longer than reason would suggest due to deeply institutionalized Western societies’ hubris about the permanency and moral superiority of their Cold War legacy control of the international system despite the overwhelming demographic and eventual economic scale of the rest of the non-western world. The ‘winners’ of the Cold War ignored the reality of their cultural uniqueness. The result was insufficient security concerns for the national wealth in their own IT capital goods manufacturing, and of the possibility that the international system they created could be contested and bested by the scale of dedicated, rising adversaries.

A. Built Fast, Cheap, and Shoddy

From its commercial outset, cyberspace was built fast and cheap in order to create a widely overpromised prosperity as quickly as possible. In the early 1990s after almost three decades of

[6] This section largely draws upon (Demchak, 2016)

development built in and for universities by public funding, cyberspace emerged for public and commercial use as the “internet”. (Hafner, 1999) It was already embedded with the ideology of a public good thereby meant to be free and benignly useful. Sharing the technological developments and access openly across universities became a social presumption embedded as intrinsic and inevitable for the generation of new ideas, languages and software. Security was an afterthought, The time-consuming, fault-intolerant coding languages used by academics were hard to hack in any case and the early networks connected to relatively few and well known small communities.[7] Furthermore, concerns were limited because early cyberspace did not uniformly connect everything important as it would grow to do twenty years later. Its challenges were unreliable transmission, some cybercrime, and possibly sociopathic organizing. (Rochlin, 1997) The bigger concern was just getting the sharing of the electronic 1’s and 0’s to be reliably transmitted across often poor electric lines. (Kinnersley, 2015)

Despite its reality as a man -made, -owned, -maintained, -updated, and -monitored, the internet spread with this presumption of being intrinsically an open, unfettered portal to access freely shared, objectively true data called ‘information.' Even though the ‘world wide web’ spread commercially by ‘Internet Service Provider’ (ISP) firms as a ‘peer or pay’[8] system of access, it acquired a new name – “cyberspace”, and was promoted with acquired almost mystical properties.[9] Barlow’s 1996 “Declaration of Independence for Cyberspace” declared all networked individuals to be ‘netizens’ beyond the reach of governments. Not by declaration or any necessary act by those individuals, but by simply entering into this connected world of such complexity and connectedness that no bureaucracy could succeed in controlling it, netizens thus freed themselves of any legacy societal constraints. (Barlow, 1996) Other and academically credible scholars said this new cyberspace would produce a world in which laws emerge from the collective consciousness without governments or national boundaries. That vision of no government presence in cyberspace became deeply embedded and continues to be subconsciously endorsed today as a basic framing — that this new digitized world village would be inevitably a universally benign, freely shared, implicitly democratic and government-free global space for good, uplifting all who connected into it.[10] (Norris & Jones, 1998)

As the computer industry fed the emerging internet frenzy through the 1990s, however, commercial interests were -- unlike their academic colleagues -- both impatient and proprietary. (McCarthy, 1978) (Mathur & Singh, 2013) By the early 1990s, the demand from the private sector to

[7] In 1995 and 1996 access to sites were shut down in Germany due to German laws on pornography and Nazi sympathizer materials. (Hughes, 1996)

[8] Peer or pay means that ISPs or other nodes will only pass through another node’s internet traffic on contractual terms, either freely as a peer or with agreements about how the transiting node is to be paid to move the traffic along. For a truly enlightening explanation of how this otherwise ignored reality of the internet operations, see (Blum, 2013).

[9] The problem of not knowing the basics about the global web continues, even among those charged with making highly consequential national policies. In 2011, at a senior level cyber policy conference, several senior US individuals offered deeply felt suggestions about governance of cyberspace. Later in the same conference, they confided to me that they did not know how the internet was actually constructed. (author personal observation) See also Singer and Friedman’s 2014 book intended to try to compensate for this appalling ignorance. (Singer & Friedman, 2014) The difficulty is that this and similar books are emerging now – twenty years on – after the developments outlined in this paper are already well advanced due in large measure to the early and widespread levels of ignorance about cyberspace as a socio-technical-economic system.

[10] Arguments for access to Wi-Fi broadband as a basic human right equivalent to the right to existence are highly normative. (Tully, 2014) (Oyedemi, 2014) A variant argument is that access to ICTs is an ‘instrumental’ human right. (Barry, 2014) See Cerf’s cogent rebuttal.(Cerf, 2012)

fund and therefore use these network tools for commercial purposes was overwhelming. The National Science Foundation -- the last official guardian of the otherwise publicly sponsored internet -- opened it up to private carriers fully by 1994. (Frischmann, 2001) From then on, the influence of commercialization on the dominant design of the web was profound. Those more secure established (1960s on) academic languages such as LISP – lengthy to code and intolerant of faults - were seen to take too long and consume too many resources for commercial revenue returns. (Trickey, 1988) Funding flowed to those computer scientists migrating from the earlier less hackable languages to those that could tolerate mistakes in code and yet perform their intended tasks, such as C+ (1990s on). (Wexelblat, 2014) With the rise of commercial interests, entrepreneurs such as Bill Gates wanted to a healthy return on his investment in software. He did not want to make sure programs were perfect before selling them -- DOS stands for 'Dirty Operating System' -- nor to have code shared widely before a return on investment could be achieved. (Rosenzweig, 1998)

The result was a commercialization tsunami with an IT capital goods business model that emphasized the rapid factory-like production[11] of standardized, fault-tolerant (more easily hacked) software getting to the market as quickly as possible.[12] (Houidi and Pouyllau 2012) Beyond login passwords to keep account ownership clear, security concerns were still chiefly reliability of performance, safety of transmission of bytes, and design efficiencies in production for the emerging markets across the US and Europe. (Anderson, 1994)

The utopian vision of a new free world of ideas and collective virtual freedom flowed readily into the commercial world of university graduates and self-taught talent, but the emerging IT capital goods industry was not particularly concerned with the imputed democratization-spreading aspect of cyberspace, only with the aspects that promised freedom from government regulation of their activities, markets, and products. Their libertarian IT capital goods industry business model was widely promoted as benign, efficient, and uniformly economically advancing for everyone. Building on a general ignorance of the techniques and physical realities underpinning cyberspace, the technically skilled in the IT world argued repeatedly that only they alone could produce the global prosperity promised in the new internet age – and only if government in particular never – ever – regulated their industry. The view blended with the utopian view that governments would wither in any case with the rising democratization to inevitably follow as people joined the internet. Quickly enough as e-commerce was promoted and enthusiasm to modernize spread, that view became taken for granted across the digitizing western civil societies' public and private communities.

For the next twenty years and until reality could no longer be ignored, western political and economic elites would determinedly argue that the Internet and all its technological designs and development were to be completely open and unfettered by regulation – in particular, something that

[11] The phenomenon of employing a large number of young programmers to whisk out standardized code as fast as possible – with the plan to fix 'bugs' later -- was particularly attributed to Gates' Microsoft with its factory like cubicles and tasks of young programmers called 'Microserfs". (Coupland, 2004)

[12] Often overlooked is the role of globalized mass production in enabling cyber predations in particular. The standardization so essential to the business model of major IT capital goods corporations such as Microsoft played a significant and role in the exceptional broad number of targets and elevated levels of economic losses to nations today. (Geer et al., 2003)

governments and borders should never touch. (Rosenzweig 1998) The threat was that, if the regulators were allowed to inhibit the freedom of the web, its prosperity – even its generativity -- would be lost.[13] Westernized communities came to view the open internet's economic benefits as explicitly tied to a lack of government controls for any reason. As a result and irrespectively of the opposition – to include a rising China, western public and business elites vigorously argued against erecting national jurisdictions across cyberspace as economically daft as well as morally unacceptable in this new cybered world.[14] (Lessig, 2004(1998 original)) Until as recently as 2011, those in the open internet community still dismissed evidence of bits and pieces of cyber national borders emerging unstoppably across cyberspace.[15] (Betz & Stevens, 2011) This devout fixation on keeping the internet globally universally open and operating along idealized democratic civil society values, however, began over time to founder on the reality that, even for unrealistic utopian visions or libertarian commercial interests, the Internet itself was simply built badly.

Rather than democracy and ubiquitous prosperity, the rapidly coded, more easily hacked programming languages creating the globally open cybered substrate offered five distinct advantages in offense that had historically only been available to emperors or close neighbors. With nearly free access to the web, predators en masse and large or small could without fear of punishment create large scale in attacking organizations (or botnets), get globally close in proximity for intelligence or reach purposes, and choose among unprecedented ranges and levels of precision in their remote operations – all for any reason including whimsy.[16] A massive underground global cybercrime market then developed with specialized submarkets, warranties, and tools including services to further enable these bad actors – and to employ them in servicing other predators. (Glenny, 2011) Two more cyber-related advantages emerged: deception in tools and opaqueness in origins. Now malicious actors could both obscure their tools – thereby using them again in a variety of other choices while avoiding the quick development of counter tools – but they could also hide themselves across nations, buried in the flood of the global web and avoid having their own local systems hacked back in punishment.

Soon enough, the underground cyber criminal community also hosted governments and transnational criminal organizations that joined into the global hacking for information, money, and political or economic leverage.[17] Over the course of the first twenty years of the global cyberspace, a

[13] The embedded nature of this threat – the loss of economic innovation if the internet's libertarian path is disrupted – continues today, especially among the more technical thinkers and practitioners. For example, “"if ISPs, diverge from the Internet tradition of the open neutral platform .... It might reduce the rate of innovation, reduce the supply of content and applications, and stall the internet's overall growth." (Clark, 2010) For an interesting nuanced concern, Zittrain cautions against the loss of human gatekeepers able to balance both generativity and security, and the potential for the rise of regulators to dampen both in the name of meeting consumer calls for security. (Shema, 2010)

[14] Buried in the thinking of even the more libertarian scholars is the notion that, while one must be left alone to use cyberspace as one likes, that use must nonetheless be standardized under open internet western rules. Clark for example argues for understanding of the developing world's “different governments with different cultures and rules and regulation, different users with different skills, … onto which we will try to impose uniform Internet standards." (Clark, 2010)

[15] It is interesting to speculate whether, had this new world been content to stay under the regimes for which its legal and value presumptions were appropriate, the web might have remained within these states as a communally shared resource subject to reciprocal laws, conveyances, and mutually agreed upon limits to surveillance for privacy reason.. (Langheinrich, 2001)

[16] For a longer discussion of these systemic advantages, see (Demchak, 2012)

[17] The global underground cybercrime black market is about 80% mid and low skilled actors who ticker with or use someone else's software program. The last 10-15% are the truly skilled coders – the ‘wicked actors’ – employed by states or

dizzying variety of predators and adversaries for a wide range of reasons emerged to threaten any open and digitally advanced nation's entire inventory of critical largescale 'socio-technical-economic systems' (STESs) and – in the process – the nation's long-term economic vitality.[18]

Over this frontier era of cyberspace, hacking has risen to such scale that digitally connected nations now face four layers of complex systems surprise. In the precyber era, states had to deal with systemic failures in two layers: first, surprises disrupting in very large, single enterprises critical to the nation, and second, rippling failures across connected sets of critical infrastructure enterprises. For thirty years, scholars in the largescale technical systems (LTS) field studies those complex surprises and even developed a set of standard responses. (Comfort, Boin, & Demchak, 2010) These challenges were large enough, but at least they were bounded by national borders. With the advent of the globally open, easily hacked cyberspace substrate, however, two more and much more poorly understood or studies major sources of national systemic surprise erupted into national systems. Now the STES digitally connecting a whole nation faces a third layer of surprise in the continuing tsunami of cyber assaults by large masses of middling skilled bad actors from across the world exploiting the five advantages of scale, proximity, precision, deception in tools, and opaqueness in origins from around the world. A fourth layer of systemic surprise developed from that huge community of malicious actors to produce a much smaller number of exquisitely skilled 'wicked' actors.[19] Their coding and hunting skills and dedication are so elevated that they are usually called 'talent' or 'advanced persistent threats' and almost always employed by criminal organizations and governments. (Demchak, 2012) (Juuso et al., 2013) (Baskerville, 2006)

Together these four layers of complex system nasty surprises and the five offense advantages helped hasten the decline of their hosting democratic civil societies. Although not recognized clearly as such, they have helped derail the promised prosperity and benign tolerance promised by the early utopians and imposed an enormous large societal cost to securing the economic wellbeing of the western states who originated cyberspace. Even what was once the dominant superpower – the United States – has found it does not have the resources to simply absorb or repel the daily onslaught of attacks by state and non-state actors.[20] Major corporations began recognizing – and finally admitting – major information losses. Some, such as Canada's Nortel, went bankrupt after theft of their critical intellectual property.[21] After only two years in office as the Director of the National Security Agency,

transnational organizations and so good that they will get through most defenses. This group includes the so-called "Advanced Persistent Threats" (APTs) generally associated with espionage, but the wicked actor group is larger because of the transnational sources can be both focused on crime as well as espionage. (Demchak, 2012) (Juuso, Takanen, & Kittilä, 2013) (Singer & Friedman, 2014)

[18] It is important to note how very recent is the realistic possibility of connecting every process to the internet and, thus, how disrupting to existing social systems. (Kopetz, 2011)

[19] Often called APTs or Advanced Persistent Threats because they are usually working for a transnational criminal organization or a government. See for example (Mandiant, 2013).

[20] (Richmond, 2011; Schrage, 2011) (Goodin, 2010) (Brian, 2010; Liff & Erickson, 2013)

[21] The Nortel Corporations bankruptcy is a major and clear case of this kind of slow roll of national knowledge stocks. Nortel went bankrupt in 2009, having been exploited by the Chinese firm Huawei in 2006-2007 due to cyber extractions of critical data, and then beat to the broadband wifi market for which Nortel was preparing its major and existential launch. In 2010, the CTO of the former Nortel was publicly listed as working for Huawei and seeking small technology startups for Huawei 'investment'. (Rogers & Ruppersberger, 2012) (McGregor, 2012) Hacking is increasingly so sophisticated

General Keith Alexander in 2012 called the losses in intellectual property and future market returns “the greatest transfer of wealth in human history.” (Paganini, 2013) The Netherlands discovered in 2012 that its 2010 GDP growth had been halved by the costs of cybersecurity and the market losses associated with the massive intrusions.[22] According to a 2014 PWC report for 2014, given the World Bank’s estimate that the entire globe’s GDP totaled $75 trillion in 2013, then the losses of trade secrets and therefore future earnings could range as high as $2.2 trillion. The effects are concentrated so far in westernized nations, shaving as much at 1% to 3% off a nation’s annual GDP. (PWC, 2014)

B. Western Hubris Delays Recognition of Changing Reality

That the reality of this shoddy construction and mounting economic losses could be ignored for almost twenty years is due to as much to an enduring western hubris fixated on the inevitability of entire world evolving along the western model, as it was to the strong utopian-libertarian blended vision of cyberspace. The peculiarly western presumption that the end state of all societies would be a democratic civil society carried on in the development of cyberspace, allowing major actors to dismiss as mere cybercrime the economic costs of unprotected resources being hacked or manipulated by organized and government-paid foreign bad and wicked actors. A disinterest in economic statecraft prevailed as well, due to an equally firm presumption that the liberal western international economic system was now so firmly ensconced that no one – no rising power of any size – could significantly overturn it. (Mastanduno, 2012) (Blanchard & Ripsman, 2008) (Demchak, 2013)

So strong was this presumption of both immortality and dominance of western governance preferences that international institutions such as the World Trade Organization (WTO, formerly GATT) became - over the western dominated era of the Cold War and aftermath - the forum in which states misbehaving economically were to be corrected. No longer would victim states need to individually engage in their own economic statecraft to change another state’s bad behavior according to collectively agreed upon rules for membership. For example, while it was known that China did not meet the basic requirements to enter the WTO in 2000, the nation was nonetheless admitted to membership with this underlying presumption that even a nation the size of China must as a matter of course eventually submit to the western economic rules. (Blancher & Rumbaugh, 2004) The presumption prevails today even though the reality says otherwise. To date, China has not met its own promises to fulfill requirements, and yet there is no discussion of ejecting the state. (R. D. Atkinson & Ezell, 2015)

This underlying western complacency about democracy has served to reinforce the utopian-libertarian conflation of conflating democracy and a lack of any government intervention in cyberspace. The three parts of this combined logic is that democracy is the inevitable end-state of all nations, an open internet inevitably democratizes any using state as long as governments leave it unfettered completely, and that any government enforced rules on IT capital goods industries will ‘balkanize’ their

that, despite the massive growth of the commercial cybersecurity industry, on average nearly a third of attacks penetrating into an organization are unstoppable. (Lumension, 2015)

[22] Melissa Hathaway, talk prepared for and delivered remotely to cyber expert workshop, at the US Naval War College, September 2015, Newport, RI.

internet (i.e., IT markets), destroying thereby its democratizing effects along with a nation's prosperity in a digital age. (Wrobel, 2013) This deeply ensconced logic has for twenty years, in particular, strongly reinforced western communities' collective opposition to legitimizing any national borders in cyberspace. (Kroker & Kroker, 1996)

With the utopian vision, libertarian IT capital goods business model, and the embedded western hubris as a trifecta, democratic governmental responses to cybered threats have been weak, derailed onto ineffective international institutions, and particularly vigorously opposed to having separate national cyber jurisdictions. The latter in particular has been held up for derision and rejection across multiple fora. (R. Atkinson & Brake, 2015) In response to data on massive cyber extractions and rising defenses, many internet governance-related forums -- GFCE, IGF, Global Commission on Internet Governance, NETmundial Initiative, WSIS, WCIT, and the GCCS 'London Process'– have nonetheless redoubled western pressures for nations to be more open to the global internet and more law-abiding, for example, applying international liberal rules internally in cyberspace. A major example is the strong push for Chinese acquiescence to United Nations (UN) human rights applied to cyberspace internally as part of the future cybered world system – a demand that China vigorously rejects as intrusion on its national sovereignty.[23]

This consistent and seemingly immutable opposition to the internal governance concerns of the authoritarian leadersenergized a major rising actor of enormous relative scale, China, to work actively internationally and economically to counter western presumptions about democracy, economic international rules, and – especially – national cyber jurisdictions. The reality is nonwestern, authoritarian actors are rapidly moving onto center stage led by China accelerated the trends in economic and international influence losses. That rise was inevitable over time, but the West lost purchase more rapidly over the international liberal economic system it built and enforced because of its own invention – the internet. Fighting the rise of national control of jurisdictions in cyberspace has distracted civil society governments and – especially -major western economic actors. They failed to recognize the indicators of a waning era of western dominance and its liberal international economic system with universal enforcement of fairness, transparency, impersonalization, and legal recourse in economic exchanges. In short, the western nations built the internet badly, viewed it inaccurately, and have proven slow to defend it – or their own long-term economic lifeblood – for over twenty years.

III. Cyber Westphalia Rises amidst Resurgent Authoritarianism for a post-western International System[24]

Cyber borders are rising globally nonetheless. The forms are varied, some in the form of tightening technological, ISP, or policy controls on traffic transiting existing national borders, others in the form of increasing monitoring and removing or rejecting of suspicious traffic that has passed into

[23] These are, respectively, the Global Forum on Cyber Expertise, the Internet Governance Forum, World Summit on the Information Society, World Conference on International Telecommunications, Global Conference on Cyberspace, among many others.

[24] Much of this discussion is drawn from (Demchak, 2016)

national servers, and yet others in the form of indirect access and content controls executed through controlled browsers, subscriptions, or identification tagging and logging. (R. J. Deibert & Crete-Nishihata, 2012) However much the western states have fought for an open and unfettered cyberspace, consolidated civil societies are also now creating – if discordantly – domestic filters, gateways, and policies for the cyberprotection of their citizen whose lives depend on the poorly secured cyber substrate.(P. J. Dombrowski & Demchak, 2014) Along with other authoritarian states,China never gave up its control on internal communications systemsand is now reinforcing its national cyber borders with newer technologies. Quite often these newer systems are built through the purchased compliance – some might say 'hypocrisy' – of many western IT capital goods firms captivated by the size of the Chinese market to which, ironically, they are never given the free access they expected in return.

China's scale, presence internationally and ability to offer technological benefits have developed a new persuasive – and nonwestern – narrative about national cyber sovereignty as possible with economic prosperity. That is, as demonstrably shown by the Chinese rise, adding borders does not 'break' the internet and destroy its generativity as western policymakers and technology private sector leaders warned. Overt and latent authoritarian national leaders have been emboldened as a result, and the Cyber Westphalian world is emerging rapidly.

A. Dismissing China's Cyber Sovereignty Accelerated Trend

Since connecting to the global Internet in the mid-1990s, China's spokespersons have consistently made its sovereignty expectation explicit – including across the internet. (Whiting, 1996) Other authoritarian leaders during the 1990s often conceded to demands for internet openness in return for the promised big economic payoffs, but China was among the earliest of the authoritarian states to clearly want both the economic benefits of an internet and a controlled internal communication system. (Kalathil & Boas, 2010) Most importantly, it was clear to Chinese leaders that avoiding any democratizing effects of the internet would require central Chinese control of its own – sovereign – web. (Qiu, 1999) (Gresh, 2008)

Even before cyberspace, this kind of pushback against the unacknowledged western hubris has never been easy. (Goldstein, 2015) From the Chinese point of view, western governments and civil society promoters consistently have refused to consider – let alone accommodate - the Chinese sovereignty demands on a host of issues for at least a hundred years, expecting democracy to break out at any moment. [25] (Bradley, 2015) For cyberspace, western political and economic leaders regarded the Chinese position as hopelessly out of date, inefficient (libertarian demand for no government control), morally wrong (access to the internet approximates a human right), and contrary to the path of history leading to a world of democracies. (Skepys, 2012) (Kalathil & Boas, 2010)

Chinese frustration at the western opposition was understandable. Given the Cold War's history with the UN in particular, the leaders of China, Russia and many other non-westernized leader could

[25] Western hubris is deeply embedded in scholars regularly declare Chinese resistance to western preferences as transitory. (Peerenboom, 2006) They have for over a century interpreted a wide variety of phenomena as indicators of progress towards the inevitable civil society model. (Bradley, 2015)

reasonably have expected that sovereign rights of a nation would be upheld for cyberspace. (Duara, 1997) Unlike space, for example, it is completely a man-made underlying substrate relying mostly on undersea cables connecting one nation's sovereign soil to another's equally sovereign territory.[26] (Blum, 2013) No one questioned the right of a nation's government to demand that transnational corporations entering that nation adhere to the local national laws in terms of taxes, environmental rules, or even human relations in hiring and firing. Indeed, linear feet upon linear feet of shelves in western book stores hold many volumes on international management and business describing how western businesses seeking to operate abroad must abide by the other sovereign nation's laws. In no other industry not directly involved in war (such as nuclear weapons) was a nation's demand for sovereignty so simply dismissed. After all, the UN – a foundation of the post-WWII liberal international system and its basic multilateral character – has routinely upheld national sovereignty. (DeNardis, 2014) If one was not taken with the optimism visions, swayed by the economic libertarianism, or imbued with western hubris, expecting sovereignty to be more or less automatic is a reasonable opening position, even for cyberspace. (Qiu, 1999)

By 2005, after roughly ten years of requests for sovereignty repeatedly rebuffed, the Chinese response was to strengthen its international campaign to alter the global narrative to accept national sovereignty in cyberspace. By this time, China's leaders had relatively better reasons to expect their campaign would be successful. For the first time since the 1990s, China was developing the economic weight to muster forces internationally and bilaterally against this western dismissal of their demand for cyber sovereignty. This campaign focused on using the influence and visibility of particular major institutions in the current international system, such as the ITU (International Telecommunications Union, hosted by the UN).[27] (Yong & Pauly, 2013) By 2011, China's leaders had positioned themselves and some allies in key influential positions in international technical organizations, and across critical IT and related markets.

Nonetheless, after another ten years, by 2015, an international endorsement of China's cyber sovereignty – let alone any other state's – by the international community still has not formally emerged. The prestigious 2011 GCCS 'London Process' international internet governance meeting, for example, once again endorsed open Internet as a human right inside every nation. For the Chinese, these western internet governance blind spots do seem to reflect a cybered form of the deafness of imperialists.[28] "America spreads the ideas of democracy widely across the world, but in cyberspace, it's the opposite," [Hao YeLi, former PLA senior official 2015l] said. "The United States continuously maintains a system to monitor the rest of the world but asks other countries to strictly control themselves and remain within bounds. This unsymmetrical line of thinking continues." (Mozur, 2015)

[26] Many cyberspace policymakers, pundits, and civil society promoters do not really know the structural and contractual basics about the global web. Such folks are often resistant to discussing the physical aspects of technology, as though it did not matter for a largescale socio-technical-economic system such as cyberspace. Singer and Friedman's 2014 book was intended to try to compensate for this appalling ignorance. (Singer & Friedman, 2014) The difficulty is that this and similar books are emerging now – twenty years on – after critical early perceptions and policy paths were already well advanced.

[27] The campaign includes exploiting the grey areas in western rules of law to benefit Chinese corporations or avoid punishment for infractions, a variant 'lawfare'. (Dunlap Jr, 2001) (Brink, 2013)

[28] This inability to accommodate the concerns of developing – read 'lesser' – nations is of very long standing, not only in cyber issues. (Hill, 2014) (Bhuiyan, 2014)

The 2016 statement by the UN's Group of Governmental Experts (GGE) for cyberspace has come the closest, but it is far from what is needed to internationally recognize a nation's cyber jurisdiction as a state's territorial sovereignty is accepted.[29] To add to the frustration, the civil society utopian promoters have since moved the terms of the debate in fighting a rearguard battle to build another obstacle. Internet governance conferences – not sponsored by China, close allies, or the UN -- now elevate the moral and efficacy value of 'multi-stakeholder' meetings -- involving states, commercial interests, and civil society groups in governance – as equal to or better than the 'multilateral' state level meetings traditionally held by the UN.[30]

As of now, the Chinese narrative has hardened publicly against the combination of cyber utopian vision, libertarian economics, and westernized concepts of civil society. (Zheng & Lye, 2015) Not only are they determined that China will have its own cyber sovereign borders, but so will other states to the extent that China's economic and international political power can ensure. China's pragmatists have expected and planned for conflicts with the US on economic, information, institutional, and cultural fronts, seen as an inevitable outcome when a current hegemon resists being displaced. (M. Liu, 2015) (Zhao, 2015) Accordingly, in the past, they muted the public challenge to western disrespect of China's rightful place. In the last few years, however, Chinese senior political and corporate leaders have escalated their aggressive use of rising economic power in cyber and other arenas. Along the way, China's political and economic leaders have learned to exploit the impunity benefits and "Teflon" legitimacy of a near superpower with a very large attractive internal market. (Rowley, 2010) For example, Chinese leaders see the 2015 Obama-Xi agreement regarding cyber-espionage as support for China's Rising Great Power narrative. Without any enforcement mechanism, the largely symbolic agreement depends on the decisions at any given moment by each party to do – or not do – as they promised. In the Chinese view, its general tolerance of poor behavior internationally constitutes the kind of accommodations made between peer great powers, (Hao, 2015)

The wider, more assertive narrative relentlessly uses the rise of China as a future great or super power to rationalize its right to question the current international system's governors. (X. Li & Shaw, 2014) The apparent objective is to influence changes in cyberspace producing a structure more convenient – or at least less threatening – to Chinese national preferences. (DeNardis, 2014) With the new narrative and its clear demonstration of an authoritarian state controlling its internet and yet rising dramatically, China's public and commercial leaders and thinkers now see an opportunity to advance more quickly and are moving to seize the opening, and bring a good portion of the nonwestern world along with them. (Kallio, 2015)

[29] See for example "New International Cyber Rules Likely Off the Table for UN Experts Group" at http://www.nextgov.com/cybersecurity/2017/02/new-international-cyber-rules-likely-table-un-experts-group/135193/

[30] The term 'multistakeholderism' is a term becoming widespread, emerging first during the ICT driven globalization surge from the 1980s- mid2000s. (Lund 2013) A strict read of democratic theory would find it odd that civil society activists would demand non-elected leaders of large corporations be given a seat in deciding the rules of interstate commerce, politics, cyberspace, and by extension, the tools of conflict. However, the key characteristic of the cyber utopian vision is its blending of individual freedoms with economic libertarian freedom and the presumption that a cybered world's prosperity depends on both of them absolutely. (Calandro et al. 2013) Ironically, however, for the IT capital goods industry, these borders and values issues are not linked. The business models only require no governmental restrictions in markets, not universal freedom of speech, and that is also fungible. Many major IT corporate leaders concede to Chinese requirements for technology transfer or surveillance compliance. (Tan and Tan 2012) (Jiang 2012) (Shih, 2014)

B. Rising Cyber Westphalia to be led by Authoritarian States

As China's narrative gains prominence and adherents, its influence rises globally. . While western states' foreign policy circles continue to fight the Chinese narrative on cyber borders, by 2017 cyber borders in praxis are being grudgingly and indirectly accepted. A wide variety of Western documents -- including the widespread rise of national cyber security strategies – recognize a government's obligation to protect their own national cyber jurisdictions. For example, when developing nations' leaders allow the Chinese firm Huawei –to build and operate their national telecommunications public agency's critical national 4G networks for nearly no upfront costs, western states are fighting a battle that they have already effectively lost. (Gagliardone, 2015) (Chung & Mascitelli, 2014) As the Chinese have argued, each bilateral agreement that acknowledges the responsibilities of another state in the parts of cyberspace connecting within their established national territory is one that in effect acknowledges the existence of national cyber jurisdictions. (J. Liu & Deng, 2010; Rowley, 2010)

Furthermore, the Chinese model of societal information control and their wider neo-capitalist business practices have a powerful resonance with the rest of the non-westernized world. (Chen, 2001) Authoritarian leaders were never enthusiastic about unfettered communications access for their citizens, yet the past twenty-five years have been difficult in terms of their national cyber sovereignty. Initially to maintain their control of societal behavior, these leaders would centralize and manage national communication networks and content, such as telephone, telegraph, and postal services, as well as radio and television. Although it would have been natural for these leaders to simply refuse the openness of the western internet, the western model of economic advancement seemed to be the only alternative to staying poor and exploited. The post-Cold War era had brought with it an international movement for to rapid economically advancement. One heavily promoted path was through the 'information revolution, especially the modernization of their aging telecommunications systems in accordance with the dominant memes of an international system guided by the economic and military dominance of the western democracies. (V. Schneider, Fink, & Tenbucken, 2005)

The nonwestern and many westernized nations accepted the orthodoxy the early internet narrative – that if they removed government controls and privatized their centralized, government owned telephone-telegraph-post agency, money would flow into their economies. (Baran, 1996) Many countries gave their agency a more commercial name with reduced formal government control, and opened up to westernized models of internet and then cell phone service. (Frischmann, 2001) Authoritarianism is the norm in political structures throughout history, especially if societies grew large and concentrated enough to requiring organizing many unwilling denizens against environmental and political challenges likely to destroy the society or, more often, its ruling classes. The approach seemed to have worked over centuries despite the lack of a civil society or human rights sensibility. As a result, many nonwestern cultures with deeply embedded authoritarian roots are better seen as finding more security in their own – rather than western civil society – political structures. (Swyngedouw, 2000) However, in the democratizing fervor of the early internet years, these nations and their leaders were not offered much of a middle ground in the western vision of the universally democratizing global cyberspace, not even the option to be sovereign within their own networks.

Although the last twenty years have been filled with noble echoes of the western views of the open internet –largely in the UN speeches -from China, its desire for surveillance and control of its citizens on the web has received support among non-western states. (R Deibert & Villeneuve, 2004) What the westernized societies interpreted as acquiescence to their democratized world view during the 1990s was really authoritarian leaders waiting to see how and when it would be safe to return to controlling their internal communications systems as they chose, without sacrificing economic gains. For example of this holding pattern, while declaring itself a democracy in the 1990s, Russia never dismantled SORM, its central communications monitoring system.(Soldatov & Borogan, 2013) Other states only superficially disengaged their governments from control of the underlying cables or telephones running the new cyberspace.

China has provided an alternate model of success to the one advanced by the western countries, a strong voice against western domination in international institutions, and alternative sources of technology and capital more suited to the desires for surveillance and interception of leaders with authoritarian tendencies. With Chinese support, they have the option of operating more aggressively on their internal internet, confident of relatively strong similarly-inclined allies outside the western dominated institutions and norms. China now routinely promotes itself in a 'globally noble'' argument to collect allies -- that the whole of the internet does not serve the equity and rights of all nations.(Bhuiyan, 2014) In response to the publicly stated western expectations that cyberspace will democratize a using society, the Chinese narrative accentuates the instability and greater dissent that can accrue with a border-spanning open internet. (Cui & Wu, 2016) It is clear unfettered public dissent can prove unhealthy for authoritarian or semi-governed states and their leaders, and this common security argument can produce allies despite apparent geostrategic differences. In 2011, Russia joined China in proposing an "International Code of Conduct for Information Security". Despite the document's resounding rejection by the West, its language formally expresses the basic desire for absolute sovereignty to be the governing principle of the international cybered system. (Farnsworth, 2011)

China's narrative also includes as legitimate sovereign cyber actions a wide range of national online societal controls online from internet surveillance to the shutdown of the domestic web as needed. Known for cutting off neighborhoods, bars, websites, and services, China prominently cut off a province in 2009 for six months in response to unrest. Its narrative clearly considers this policy to be within the sovereign right of a nation to do so. (MacKinnon, 2011) While many developing authoritarian or unstable nations duly privatized their main telecommunications agency in the 1990s, they are now rediscovering that they may nonetheless use the central position of these telecommunications firms for online censorship, access control, surveillance, throttling of traffic, or outright cut offs of whole population segments .(Ronald Deibert, Palfrey, Rohozinski, & Zittrain, 2012) Sometimes it only takes phone calls as happened in Egypt in the Arab Spring. [31] (Shin, 2015) Increasingly, however, national leaders are acquiring the technological means to selectively target whole regions to isolate from the internet. (West, 2016) In 2017 between January and April, Cameroon cut two regions from the internet for 94 days to quell dissent by the English speaking 20 percent of its population against the imposition of the French language in schools and courts.[32]

This pattern – inconceivable when the global web was solely a western reserve – is growing especially among nations more inclined to authoritarian rule and cyber sovereignty. Afrinic (one of five global IP address block allocators) has tabled a proposal to punish governments with no new IP addresses if governments execute a shut down. The measure has little chance of being adopted in the next Afrinic meeting in June 2017 in Kenya.[33] China, India, Russia, Kenya, and others nations are opposed. With the Chinese telecommunications giant Huawei building much of the critical cellular communication structures of Africa and bringing a Chinese perspective on the extent of technological sovereignty these nations should enjoy, few of the continent's governments need choose in advance to give up the right to use that technological lever if they see the need.[34] Huawei – as well as not a few 'flexible' western IT capital goods firms – will build these options into the communications backbone of a nation if so desired. In addition and at the moment, allying oneself as a closer friend to China – as opposed to the United States in particular – tends to reward a national leader with Chinese promises of infrastructure investment in large amounts – as the leader of the Philippines has recently demonstrated.[35] (Duanmu, 2014)

At the end of the day, borders ARE rising as defended cyber jurisdictions across authoritarian and nonauthoritarian states, with even the formally opposed western democratic civil societies building their own cyber borders in bits and pieces. Despite the formal foreign policy language of western states still strongly calling for a globally free and open borderless internet, the domestic policy language of concern by westernized government is now riddled with references to defending their domestic cyberspace, rising from highlighting solely cybercrime, to more broadly critical infrastructure protection, and now to losses to the entire economy over time. Among most major western states, cyber security is now labeled a tier 1 or national threat.[36] Even nations known for their civil society—Sweden for

[31] It is a mistake to underestimate the negative demonstration effects on authoritarian or beleaguered political leaders when they consider the longer term consequences of a cyberspace-enabled Arab Spring–like dissent movement. (Stewart, 2013)

[32] For a set of articles on Cameroon, see https://techpoint.ng/2017/04/24/cameroon-government-restores-internet/) and (http://www.pewglobal.org/2015/04/15/cell-phones-in-africa-communication-lifeline/.

[33] See https://www.theregister.co.uk/2017/04/12/no_ip_addresses_for_countries/

[34] See http://www.cnn.com/2012/10/04/tech/mobile/africa-mobile-opinion/ and http://www.thisisafricaonline.com/News/Huawei-looks-to-Africa-to-cut-network-deals?ct=true

[35] See http://www.straitstimes.com/asia/se-asia/duterte-plans-to-diversify-economy-with-heavy-china-aid

[36] The United Kingdom is arguably the first major westernized state to declare cyberspace threats to be in the top tier of national security threats. (Norton-Taylor, 2010) The tier language has become a cross-Atlantic term of art indicating the level of importance a state attaches to defending itself in cyberspace.

example – have taken steps domestically to monitor[37] what enters or leaves their national territories networks – i.e., to defend their domestic cyber jurisdiction.[38]

However, the reality of an emerging global cyber Westphalia is not being framed in values or conflict potential by the bits and pieces of cyber jurisdictions being constructed in these democratic societies. Rather, due to the western states being distracted, obdurate, complacent, and arrogant for the first twenty years of cyberspace, Chinese technology companies, economic tradecraft, authoritarian sovereignty narrative, and international institutional successes are constructing the emerging world of cyber-bordered states that will create a new topology distributing power across the globe.

IV. Defense in Scale through Cyber Resilience Alliance[39]

Scale in demographics and markets is the Achilles heel of consolidated democratic civil societies, especially in today's cybered conflict and particularly since they are so doggedly unable to recognize it. The post-Cold War legacy inability to recognize the power of scale in system-vs-system conflict is particularly dangerous for the future wellbeing and global influence of modern democratic civil societies. As the borders of cyber jurisdictions rise in a Cyber Westphalian world structure, these societies will be - in demographic and eventually market terms – a minority. Depending on where one places nations with corruption and increasingly authoritarian politics, the democracies that are truly consolidated into stable, rule of law-bound, civil society cultures in practice as well as name across their national STES are few, totally between 30 – 40 [40] This small number compared to the 190-odd recognized nations of the world will not be able to enforce or maintain the liberal international economic system over time when the other ninety percent of the globe's population are likely to be led by the practices, preferences, and products of China and Asia for most of the rest of this century.

In any case, it will be increasingly tough for westernized civil societies to obtain and maintain allies since they are already seen to be in decline. In the 1980s, the former leader of China Deng Xiaoping predicted China would equal the US as a global great power over a period of roughly 70 years because of its demographic and economic weight in the global system. (J. Liu & Deng, 2010) By most measures, the rise of China was inevitable but has occurred faster than anticipated. Analyses, such as the 2007 Goldman Sachs estimate, predicted parity would occur by 2025, with China doubling that of the US by 2050. As of this writing, various authors argue that China has been roughly at parity for several years (at least since 2014). (M. Liu, 2015) (Fujita & Thisse, 2013) (Scott & Sam, 2016). With its poorly secured global pathways across poor and wealthy national STESs, cyberspace and its own form of "hidden hand of economic coercion" shortened that anticipated transition dramatically – to fifteen to twenty years. (Drezner, 2003) (Weede, 2015) This Internet governance challenge to civil society

[37] It is important to note that filtering is not the same as monitoring. The former removes data access; the latter notes the data's movements and possibly the content. Another way to view the difference is to note that NSA has been accused of monitoring, while China is shown empirically to filter. (Greer, 2010) (Xu, Mao, & Halderman, 2011)

[38] The law assigning this mission and authority to the Swedish Federal Police passed in 2008. (Irion, 2009)

[39] This section draws heavily from a previous publication. See (P. Dombrowski & Demchak, 2015).

[40] The role of India as a largescale nonwestern democracy likely to be critical in improving the odds for the long-term survival of democracies globally is woefully understudied. It is not included in this eleven percent figure. (Stuenkel, 2013)

presumptions is only the beginning of a host of looming multi-domain contests. If these democracies – and their economic sectors – refuse to recognize their loss of dominance[41] and to face the implications of the rise of an authoritarian much larger world – especially the need to be as systemically resilient in the face of cyber coercive peace as one used to be prepared for destructive wars, then these contests are more likely to be lost in the future.[42]

Being a billion plus population that is centrally led and nationally self-identified as 'Han' is a major advantage in scale for China across the global cyberspace substrate along the entire spectrum of cybered conflict from peace to war. China's Middle Kingdom rulers are fully mindful that their "rightful place" in the world rests fundamentally on their demographic weight as a coherent state actor in a world of many smaller nations. For China, a true peer power for the longer term must be able to coherently wield the power of a similar demographic weight. India has the demography but by far not the coherence. The US and each of its allies taken alone are by no stretch peer powers. Rather, the more they concern themselves entirely with their own cyber security and economic protection, the more they are simply opponents to eventually be over taken as China rises to its 'proper position' globally. Irrespective of what the individual democratic societies prefer, China's state economic champions have the scale and the national support necessary to build the future global internet with Chinese influence embedded across all the future population and economic concentrations of the world – and without western sensibilities, values, and eventually markets. (Khanna, 2009)

If the current trends are not altered, then China's preferences will majorly frame how this new nonwestern world will be governed; however, China has not given details of what, ideally, its leaders would like to see in place. For a state the size of China, the current and future potential to directly influence the cyber and economic preferences of the developing world – and thereby the bulk of the globe's states and populations – is enormous, and this gap in stated vision or intentions is unsettling. The Chinese narrative in speeches and publications connects this essential element -- state cyber sovereignty -- with a world where China rises to its proper place (defined by its demographic scale) as the first great cybered power that is benignly 'nonhegemonic'. The term is used to mean no state including China as rising world power will tell any other state how to operate internally. Thus, one thing is clear – this envisioned new world neatly eliminates the US as the old style global internet hegemon -- and its civil society preferences -- from the center of the global international system's governance. (Kivimäki, 2014)

Beyond that, one must look to both recent history and long cultural tendencies for indicators of how a China-dominated international system might operate. In Chinese society, its organizations, and its business practices, hierarchy is preferred uniformly, size makes right – the big are entitled to compel the small, and history trumps law unless the law's verdict suits the preferences of the one at the top of

[41] Increasing the sense of surprise that could feed outrage and poorly considered policies in the future democratic societies is a largely American international relations literature largely silent on adapting to the serious possibility of US decline. (Friedman, 2010)

[42] For a particularly in-depth and instructive comparison of how 'cyber ready' many states are, see the Cyber Readiness Index created by Melissa Hathaway. www.potomacinstitute.org/academic-centers/cyber-readiness-index

the hierarchy, i.e., China.[43] (Kardon, 2017) How China conducts business and politics inside China is how its firms and political leaders will feel comfortable conducting business and politics when China occupies the center of demographic and economic circles globally. In the past few years, China's new leader Xi Jinping and official media outlets have increasingly openly rejected civil society "western" values – chief among them freedom of speech -- and more aggressively asserted the downsides of continuing US dominance of the web. (Kemp, 2015)

In other indicators, as the economic weight of the Chinese market has grown, so has Chinese willingness to use its size in economic statecraft (and blatantly violate the WTO norms) to alternate between bribing and bullying those who do not comply with Chinese preferences, including publicity. (Kennedy, 2006) In direct and many indirect forms, Chinese leaders have successfully curtailed the libertarian demands of western IT capital goods industrial leaders over time. Threatening access to the large Chinese market has the practical effect of inducing compliance from major western corporate and political actors. Both are rewarded for accommodating behaviors explicitly from trade promises to easing of policies – at least for as long as their technology transfer or political influence is needed. (Emmott & Blanchard, 2017) For example, in 2008 Apple's founder, Steve Jobs, conceded to the Chinese demand that a heavily encrypted WAPI Wi-Fi chip of Chinese design and making be inserted in all Apple iPhones if any were to be sold in China itself. Since Jobs did not want to make two world phones, by 2009 he accepted the Chinese explanation that the chip could only be turned on and access inside Chinese borders, though it is not publicly knowable if that restriction is actually accurate. (H.-W. Liu, 2017) (M. Li, Liu, & Reimers, 2011) While aggressively demanding freedom from government controls in western states lest the commercial generativity be destroyed, many IT industrial leaders have nonetheless abandoned their oft stated (in western settings) concerns for either democracy or non-interference from governments in order to preserve their firm's access to markets in China and other authoritarian states.

One need not be the actual offending actor to catch the wrath. Non-accommodating national policies, public statements, or even unflattering news reports are punished by "difficulties" imposed on other members of the offending community within Chinese reach, whether it is the actual actor who caused offense or just other prominent members. (Reilly, 2013) Foreign companies that are seen to embarrass China are compelled to apologize, even if the actors causing the harm were Chinese employees in China far from the senior leaders, as the CEO of the toy company Mattel was obliged to do. (Story, 2007) Those who do not comply – such as Google – have been forced to withdraw (for some time) from Chinese markets and subjected to intense competitive pressures directly and indirectly. (Helft & Barboza, 2010) For example, recently major South Korean firms have suddenly experienced 'difficulties' in their Chinese operations when South Korea and China relations hit a downturn. (Jin, 2017)

What is to be done? None of this global topological change was anticipated by early internet promoters, nor desired today by leaders and citizens of consolidated democratic civil societies. Put more colloquially, how will these nations in the demographic and coming economic minority individually

[43] There is considerable speculation on what happens in the post-western world. See for example (Jacques, 2012).

avoid being vassals over time in a conflictual, largely authoritarian, cybered world. Scale needs to be met by scale, or the challenger needs to change the conditions of key aspects of the competition. In this case, changing the conditions will take longer and is less certain than the one feasible alternative available to these societies – creating the necessary scale in an institutionally and technologically integrated cyber systemic resilience alliance. It must be one that accepts the rise of cyber sovereignty among nations which will not in the foreseeable future be civil societies – if ever. Yet this alternative must preserve some remnant of the free and open cyberspace created by the West for its own tolerant cultural preferences, transparent legal regimes, and comparative well-being. And it must succeed eventually in re-making the underlying substrate properly – transforming it technologically, societally, and economically as it was intended, and defending it, even if only for themselves. The alternative is to eventually concede to a global version of China's "info-web" internet. (F. Schneider, 2015)

V. Conclusion: Creating this Alliance requires Essential Recognitions

First, a major part of the necessary response is to alter the cognitive framing created in the early frontier era of cyberspace and explicitly accept the rise of Cyber Westphalia. It has been costly for the western democracies to be so distracted into pushing for a future fully democratized, borderless, and civil society-led world that had nearly no chance of emerging. Chances to slow this rise of cybered conflict have been squandered across a range of missed technological transformation, societal resilience, markets reform, and informed policy opportunities. That doggedly western civil society narrative now has a major counter-narrative – well funded, covertly reinforced, and overtly widely promoted from a rising and confident large authoritarian actor, China – about changing the realities governing the future cybered world. Cyber jurisdictions are emerging whether or not the westernized world desires them, and opposing the process accelerates the likely affiliation of the rest of the world with the Chinese model.

Recognizing a national cyber jurisdiction – the essence of cyber sovereignty – is the first step to developing a consensus of society much like a cooperative enterprise worthy of defending in terms of its STESs' viability and political freedoms. Without this recognition, democratic leaders cannot use "stateness" [44] – a sense of collective willingness to act – in order to create and sustain systemic resilience. While cyber sovereignty has been repeatedly rejected by western corporations and political leaders for commercial and optimistic reasons, a wide array of autocratic leaders - led by China as the rising center of economic and demographic power – argue strongly in favor of internet sovereignty.[45] Those nations will – to the extent possible – have the internal coherence in power, infrastructure, and citizen/commercial entity controls to create resilience as they interpret it,[46] leaving the democratic

[44] Put differently, stateness is the ability to persuade the leaders of a state to act together to resist external coercion. See (Blanchard & Ripsman, 2008)

[45] Kissinger observed that, in his long experience, most Asian states in particular have not ever been willing to concede local sovereignty unless forced to do so. (Kissinger, 2015) p.179. See also (Chang, 2014).

[46] Nationally controlled radio stations and telephone exchanges have long been prime points of societal control in non-western states, with the internet quite unlikely to be regarded much differently in the view of national leaders – if the means to control in the same way were available. (Glanz & Markoff, 2011) (Gumede, 2016)

societies with no examples of success in doing so unless – as improbably as it sounds – these nations regain control of the entire global web and its use policies.

Second, this cyber resilience alliance will need this "stateness" as a shared identity across consolidated democracies. Rather than seeing the rest of the world as moving inexorably to becoming democratic civil societies, recognizing the cultural peculiarity – and consequent numerical fragility – of the democratic experiment in comparison to the more normal, authoritarian, and affective speaking cultures of the rest of the world will be essential. The alliance will need a common perception that it matters to each of us and each nation to defend the democratic civil societies against the economic losses and political intrusions of the rising and much larger authoritarian world. This unusual community of nations empowered by the United States grew to dominate the world when China and Russia (and allies) so helpfully self-isolated during the Cold War. They were helped by the way Russia's communism provided a discernible and distinct face of authoritarianism against which they could unite, unlike the generalized rise of authoritarianism emergent today. After the Cold War, however, these states still expected their global dominance to continue and never recognized it as both shallow and culturally incompatible with most of the world. Led by American hubris in particular, the western powers thought – and continue to think – of themselves as the universal exemplar of normal humans, not as what they are: the product of a highly and narrowly unique blend of historical trends involving Catholic transnationalism, Protestant leveling ethics, and the Enlightenment. (Goldstein, 2015; Tilly & Ardant, 1975)

Third, the alliance requires recognition of the power of demographic scale as the only measure recognized by China to merit peer status. China is unlikely to daunted, deterred, or deflected over time by this ten-eleven percent of the world's population found in democratic societies if they stand disunited, individually small in demographic and eventually market comparisons, and attempt to individually defend their own national cyber jurisdictions. They have little chance of independently gathering the necessary levels of investment and domestic talent needed to be a robust cyber power. The maintenance of secured national STESs will be unsustainable systemically if every state alone is to afford and orchestrate advanced technologies, resilience budgets,[47] and collective intelligent choices as a minority democracy in a much larger, deeply cybered, and overwhelmingly authoritarian world system.

Fourth, the alliance is feasible. The community estimated at 30-40 states has collectively about 800-900 million people in well-educated modern communities, sufficient to be relatively economic autarkic if need be and certainly capable of developing the talent and technology to compete as a peer cyber power with China if they – like China – were a unified community. The collective scale of these cultural and trade allies can be turned in their advantage in a cybered world if these minority states create a coherent entity able to defend these cybered STESs jointly. There is nothing magical about the authoritarian turn to the telecommunications agencies in those nations in order to deepen authoritarian controls. Consolidated democratic civil societies also have central telecommunications firms to be

[47] Constrained budgets easily sideline advanced technologies today, even before the era of system-wide national IT R&D and transformational deployment budgets has fully emerged. See (Cava, 2017)

enlisted into the resilience of their community. But democracies also have the large private sector likely to lose both their access to large markets in the future and their own viability as borders close and internal national policies extract technologies and concessions for access. It is not always recognized that the private sector and their talent in democracies have as much to lose with the loss of the international liberal economic system as have the nations they call home.

Furthermore, that one has yet not seen this kind of cross-border, culturally like-minded, operationally active, public and private joint resilience structure is not an argument against the alliance. One had never seen a NATO, an EU or even the anti-Confiker private sector group formed in 2009 before these structures – large and small, military, economic, and technological – were created as the need arose. One has seen remarkable organizational efforts in short periods of time if the urgency is both clearly communicated and a program to solve it collectively funded. At the end of the 1970s, miniaturization went from a strong interest of the western militaries, especially the US, to a critical major push when the Soviet military conventional buildup was seen as an overwhelming scale advantage over Western Europe. The result is a technological transformation found all around us in smart phones and other advanced technologies. The same kind of transformation is needed now, but we do not have the stability of the basic competition present between NATO vs Warsaw Pact to buy time. The alliance is needed in the near term to create the jointly defended resilience buffering the democratic societies while their collective talent innovate a new more secure and yet democratic cyber substrate and their leaders learn how to maneuver, trade, and defend in an overwhelmingly authoritarian world.

At the end of the day, the likeminded have the economic, technological, and demographic resources to stand up to the much larger scale of an authoritarian world led by China over the coming century – IF they create this skillfully integrated and operational alliance of mutual systemic cyber resilience recognizing the existential long term trends and competently defending the interlinked STESs. Alone, none of these nations will do well over time. Together, these consolidated democratic civil societies – including all the major public and private actors – can jointly muster the resources and talent to defend their entire community and values across the full range of cybered conflict. In changing the current trends, they have the chance to survive collectively as robust cyber powers adequately prosperous in trade and wellbeing, and still be consolidated democracies over the long term.

Bibliography

Anderson, R. J. (1994). Liability and computer security: Nine principles *Computer Security—ESORICS 94* (pp. 231-245): Springer.

Atkinson, R., & Brake, D. (2015). Net Gains: A Pro-Growth Digital Agenda. *Democracy*(36), 9.

Atkinson, R. D., & Ezell, S. (2015). False Promises: The Yawning Gap Between China's WTO Commitments and Practices. Washington DC: Information Technology and Innovation Foundation.

Baran, N. (1996). Privatization of telecommunications. *Monthly Review, 48*(3), 59.

Barlow, J. (1996). A Declaration of the Independence of Cyberspace. *Humanist - Buffalo, 56*(3), 18-19.

Barry, J. J. (2014). *Don't Be Evil: Should Access to the Internet Be Conceptualized as an Instrumental Human Right?* Paper presented at the American Political Science Association 2014 Annual Meeting Paper.

Baskerville. (2006). Hacker Wars: E-Collaboration by Vandals and Warriors. *International Journal of e-Collaboration, 2*(1), 16.

Betz, D. J., & Stevens, T. (2011). Chapter two: Cyberspace and sovereignty. *Adelphi Series, 51*(424), 55-74.

Bhuiyan, A. (2014). *Internet governance and the global south: demand for a new framework*: Palgrave Macmillan.

Blanchard, J.-M. F., & Ripsman, N. M. (2008). A political theory of economic statecraft. *Foreign Policy Analysis, 4*(4), 371-398.

Blancher, M. N. R., & Rumbaugh, M. T. (2004). IMF: China - international trade and WTO accession: International Monetary Fund.

Blum, A. (2013). *Tubes: A Journey to the Center of the Internet*: HarperCollins Publishers.

Bradley, J. (2015). *The China mirage: The hidden history of American disaster in Asia*: Hachette UK.

Brian, A. (2010). *Seven deadliest USB Attacks*. Burlington, MA: Syngress Media Inc.

Brink, G. F. (2013). Anti-dumping and China: three major Chinese victories in dispute resolution.

Cava, C. P. (2017, February 6). Grounded: Nearly two-thirds of US Navy's strike fighters can't fly, *Defense News*

Cerf, V. G. (2012). Internet access is not a human right. *New York Times, 4*, 25-26.

Chang, A. (2014). Warring State: China's Cybersecurity Strategy http://www.cnas.org/chinas-cybersecurity-strategy#.VeHZlM5RErs: Center for New America Security.

Chen, M.-J. (2001). *Inside Chinese business: A guide for managers worldwide*. Cambridge, MA: Harvard Business Press.

Chung, M., & Mascitelli, B. (2014). Huawei's Battle: Cold War or Commercial War? *Asian Business and Management Practices: Trends and Global Considerations: Trends and Global Considerations*, 107.

Clark, D. (2010). Fighting over the Future of the Internet. *IEEE Internet Computing, 10*, 22-23.

Comfort, L., Boin, A., & Demchak, C. (Eds.). (2010). *Designing Resilience: Preparing for Extreme Events*. Pittsburgh: University of Pittsburgh Press.

Coupland, D. (2004). *Microserfs*: HarperCollins UK.

Cui, D., & Wu, F. (2016). Moral goodness and social orderliness: An analysis of the official media discourse about Internet governance in China. *Telecommunications Policy, 40*(2-3), 265-276.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). *Access contested: security, identity, and resistance in Asian cyberspace*: The MIT Press.

Deibert, R., & Villeneuve, N. (2004). Firewalls and power: An overview of global state censorship of the Internet. *Human rights in the digital age. London: GlassHouse*.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance: A Review of Multilateralism and International Organizations, 18*(3), 339-361.

Demchak, C. C. (2010). Conflicting Policy Presumptions about Cybersecurity: Cyber–Prophets, –Priests, –Detectives, and –Designers, and Strategies for a Cybered World". *Atlantic Council Issue Brief*.

Demchak, C. C. (2012). Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World. In N. B. a. J. Price (Ed.), *Securing Cyberspace: A New Domain for National Security*. Washington, DC: The Aspen Institute.

Demchak, C. C. (2013). Economic and Political Coercion and a Rising Cyber Westphalia. In K. Ziolkowski (Ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (pp. 595-620). Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Demchak, C. C. (2016). Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age. *The Cyber Defense Review, 1*(1).

DeNardis, L. (2014). *The global war for internet governance*: Yale University Press.

Diamond, L. J. (1994). Toward democratic consolidation. *Journal of Democracy, 5*(3), 4-17.

Dombrowski, P., & Demchak, C. C. (2015). Thinking Systemically about Security and Resilience in an Era of Cybered Conflict. *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, 367.

Dombrowski, P. J., & Demchak, C. C. (2014). Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs, special issue on cyber*.

Drezner, D. W. (2003). The hidden hand of economic coercion. *International Organization*, 643-659.

Duanmu, J.-L. (2014). State-owned MNCs and host country expropriation risk: The role of home state soft power and economic gunboat diplomacy. *Journal of International Business Studies, 45*(8), 1044-1060.

Duara, P. (1997). Transnationalism and the predicament of sovereignty: China, 1900-1945. *The American Historical Review*, 1030-1051.

Dunlap Jr, C. J. (2001). *Law and military interventions: preserving humanitarian values in 21st century conflicts*. Paper presented at the Humanitarian Challenges in Military Intervention Conference, Washington, DC.

Emmott, R., & Blanchard, B. (2017, March 28). Wary of Trump, China launches EU charm offensive: diplomats, *Reuters,* pp. http://www.reuters.com/article/us-eu-china-idUSKBN16Z22S.

Farnsworth, T. (2011). China and Russia Submit Cyber Proposal ["International code of conduct for information security"]. *Arms Control Today*, 35-36.

Friedman, G. (2010). *The next 100 years: a forecast for the 21st century*: Anchor.

Frischmann, B. (2001). Privatization and Commercialization of the Internet Infrastructure. *Columbia Science and Technology Law Review, 2*(1), 1-70.

Fujita, M., & Thisse, J.-F. (2013). *Economics of agglomeration: cities, industrial location, and globalization*: Cambridge university press.

Gagliardone, I. (2015). China and the Shaping of African Information Societies. *Africa and China: How Africans and Their Governments are Shaping Relations with China*, 45.

Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C. P., Quarterman, J. S., & Schneier, B. (2003). CyberInsecurity: The cost of monopoly *CyberInsecurity Reports*. http://www.totse2.net/totse/en/technology/computer_technology/cyberinsecurit171812.html (original http://www.ccianet.org/papers/cyberinsecurity.pdf): Computer and Communications Industry Association (CCIA).

Glanz, J., & Markoff, J. (2011, February 15). Egypt Leaders Found 'Off'Switch for Internet, *The New York Times,* p. online.

Glenny, M. (2011). *Dark Market*. New York: Random House.

Goldstein, L. J. (2015). *Meeting China halfway: How to defuse the emerging US-China rivalry*: Georgetown University Press.

Goodin, D. (2010, January 14). IE zero-day used in Chinese cyber assault on 34 firms: Operation Aurora unveiled, *El Register*. Retrieved from http://www.theregister.co.uk/2010/01/14/cyber_assault_followup/

Greer, J. N. (2010). Square legal pegs in round cyber holes: The NSA, lawfulness, and the protection of privacy rights and civil liberties in cyberspace. *J. Nat'l Sec. L. & Pol'y, 4*, 139-154.

Gresh, A. (2008). Understanding the Beijing consensus. *Translated by Stephanie Irvine. Le Monde Diplomatique English Edition*.

Gumede, W. (2016). Rise in Censorship of the Internet and Social Media in Africa. *Journal of African Media Studies, 8*(3), 413-421.

Hafner, K. (1999). *Where Wizards Stay Up Late: The Origins of the Internet*: Simon and Schuster.

Hao, Q. (2015). China Debates the 'New Type of Great Power Relations'. *The Chinese Journal of International Politics, 8*(4), 349-370.

Hathaway, M. (2013). Cyber readiness index 1.0. *Great Falls, VA: Hathaway Global Strategies LLC*.

Helft, M., & Barboza, D. (2010). Google shuts China site in dispute over censorship. *NY TIMES, Mar, 22*.

Hill, R. (2014). *Internet governance: the last gasp of colonialism, or imperialism by other means?* : Springer.

Hughes, K. A. (1996). Copyright in Cyberspace: A Survey of National Policy Proposals for On-line Service Provider Copyright Liability and an Argument for International Harmonization. *Am. UJ Int'l L. & Pol'y, 11*, 1027.

Irion, K. (2009). Privacy and security International communications surveillance. *Communications of the ACM, 52*(2), 26-28.

Jacques, M. (2012). *When China rules the world: The rise of the middle kingdom and the end of the western world [Greatly updated and expanded]*: Penguin UK.

Jin, H. (2017, April 3). Hyundai flags weaker China sales after missile row; Kia's March China sales halved: source, *Reuters,* pp. http://www.reuters.com/article/us-southkorea-autos-china-idUSKBN17511C.

Juuso, A. M., Takanen, A., & Kittilä, K. (2013). *Proactive cyber defense: Understanding and testing for advanced persistent threats (APTs).* Paper presented at the Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013.

Kalathil, S., & Boas, T. C. (2010). *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Washington DC: Carnegie Endowment.

Kallio, J. (2015). Dreaming of the great rejuvenation of the Chinese nation. *Fudan Journal of the Humanities and Social Sciences, 8*(4), 521-532.

Kardon, I. B. (2017). *Rising Power, Creeping Jurisdiction: China's Law of the Sea (dissertation manuscript)*. Ithaca, NY.: Cornell University.

Kemp, T. (2015, July 6). China leaders oppose 'universal values,' but it may not matter: interview with Prof Steinfeld Brown University, *CNBC.com*.

Kennedy, S. (2006). The political economy of standards coalitions: Explaining China's involvement in high-tech standards wars. *Asia Policy, 2*(1), 41-62.

Khanna, T. (2009). Billions of entrepreneurs: How China and India are reshaping their futures and yours. *Strategic Direction, 25*(10).

Kinnersley, B. (2015). A Chronology of Influential [computer] Languages, The [Computer] Language List: Collected Information On About 2500 Computer Languages, Past and Present. Retrieved 2015 August 21, from University of Kansas

Kissinger, H. (2015). *World order*: Penguin Books.

Kivimäki, T. (2014). Soft power and global governance with Chinese characteristics. *The Chinese Journal of International Politics, 7*(4), 421-447.

Kopetz, H. (2011). Internet of things. In H. Kopetz (Ed.), *Real-time Systems* (pp. 307-323): Springer.

Kroker, A., & Kroker, M. (1996). Code Warriors. *CTheory.net*, 2-7.

Langheinrich, M. (2001). Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems. *LECTURE NOTES IN COMPUTER SCIENCE*, 273-291.

Lessig, L. (2004(1998 original)). The laws of cyberspace. In R. A. Spinello & H. T. Tavani (Eds.), *Readings in Cyberethics* (pp. 134-145). Sudbury, MA: Jones and Bartlett Learning.

Li, M., Liu, X., & Reimers, K. (2011). *Emerging mobile platform competition in China's 3G era and beyond.* Paper presented at the Service Systems and Service Management (ICSSSM), 2011 8th International Conference, June 25-27, 2011, Tianjin, China.

Li, X., & Shaw, T. M. (2014). “Same Bed, Different Dreams” and “Riding Tiger” Dilemmas: China’s Rise and International Relations/Political Economy. *Journal of Chinese Political Science, 19*(1), 69-93.

Liff, A. P., & Erickson, A. S. (2013). Demystifying China's Defence Spending: Less Mysterious in the Aggregate. *The China Quarterly, 216*, 805-830.

Liu, H.-W. (2017). Inside the Black Box: Political Economy of the Trans-Pacific Partnership’s Encryption Clause. *Journal of World Trade, 51*(2), 309-333.

Liu, J., & Deng, B. (2010). America Hegemony: Is It To Decline or To Continue. *Pacific Journal, 1*, 1-8.

Liu, M. (2015). *The China Dream: Great Power Thinking & Strategic Posture in the Post-American Era*.

Lumension. (2015). 2015 Sixth Annual State of the Endpoint Cybersecurity Survey *Annual State of the Endpoint Cybersecurity Survey*.

https://www.lumension.com/Lumension/media/graphics/Resources/2015-state-of-the-endpoint/2015-State-of-the-Endpoint-Whitepaper-Lumension.pdf: Ponemon.

MacKinnon, R. (2011). China's" networked authoritarianism". *Journal of Democracy, 22*(2), 32-46.

Mallery, J. C. (2011 (2009)). *A Strategy for Cyber Defense (earlier title: Multi-spectrum Evaluation Frameworks and Metrics for Cyber Security and Information Assurance)*. Paper presented at the MIT/Harvard Cyber Policy Seminar,, Cambridge, MA.

Mandiant. (2013). APT1: Exposing One of China's Cyber Espionage Units. In M. I. Center (Ed.). New York: Mandiant.

Mastanduno, M. (2012). Economic statecraft. *Foreign Policy: Theories, Actors, Cases*, 204.

Mathur, A., & Singh, K. (2013). Foreign direct investment, corruption and democracy. *Applied Economics, 45*(8), 991-1002.

McCarthy, J. (1978). History of LISP. *History of programming languages I*, 173-185.

McGregor, J. (2012). No Ancient Wisdom, No Followers‖: Prospecta Press, Westport.

Mozur, P. (2015, September 29). Chinese Official Faults U.S. Internet Security Policy [Ms. Hao YeLi], *New York Times*.

Norris, P., & Jones, D. (1998). Virtual democracy. *Harvard International Journal of Press Politics, 3*, 1-4.

Norton-Taylor, R. (2010, October 18). The UK is under threat of cyber attack, the national security strategy says- Home secretary outlines priority threats facing Britain ahead of the publication of the national security strategy today, *Guardian Online*.

Nye, J. S. (2014). *The Regime Complex for Managing Global Cyber Activities*. http://www.cigionline.org/publications/regime-complex-managingglobal-cyber-activities: Ourinternet.org Retrieved from http://www.cigionline.org/publications/regime-complex-managingglobal-cyber-activities.

Oyedemi, T. (2014). Internet access as citizen's right? Citizenship in the digital age. *Citizenship Studies*, 1-15.

Paganini, P. (2013). Cyber-espionage: The greatest transfer of wealth in history. *H+ Magazine online*.

Peerenboom, R. (2006). Law and development of constitutional democracy: Is China a problem case? *The ANNALS of the American Academy of Political and Social Science, 603*(1), 192-199.

PWC. (2014). Global State of Information Security® Survey 2015 *Annual State of Information Security Survey*. http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml: Price Waterhouse Cooper.

Qiu, J. L. (1999). Virtual censorship in China: Keeping the gate between the cyberspaces. *International Journal of Communications Law and Policy, 4*(Winter), 1-25.

Reilly, J. (2013). China's economic statecraft: turning wealth into power. *Lowy Institute for International Policy*.

Richmond, R. (2011, April 2). The RSA Hack: How They Did It, *New York Times*.

Rochlin, G. (1997). *Trapped in the Net: The Unanticipated Consequences of Computerization*. Princeton Princeton University Press.

Rogers, M., & Ruppersberger, C. D. (2012). *Investigative report on the US national security issues posed by Chinese telecommunications companies Huawei and ZTE: A report*. Washington DC: US Government Press.

Rosenzweig, R. (1998). Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet. *American Historical Review*, 1530-1552.

Rowley, C. (2010). Commentary: China's chimera: miracle or mirage in the ‘Middle Kingdom’? *Asia Pacific Business Review 16*(3), 269-271.

Schneider, F. (2015). China’s ‘info-web’: How Beijing governs online political communication about Japan. *New Media & Society*, 1-21.

Schneider, V., Fink, S., & Tenbucken, M. (2005). Buying Out the State: A Comparative Perspective on the Privatization of Infrastructures. *Comparative Political Studies, 38*(6), 704-727.

Schrage, M. (2011, May 6). How Amazon or Apple Could Cause a War with China: Networked and cloud-based digital businesses are vulnerable targets for cross-border mischief that could cause international conflict, says Michael Schrage *Harvard Business Review*.

Scott, M., & Sam, C. (2016, May 12). China and the United States -Tale of Two Giant Economies, *Bloomberg.com*. Retrieved from https://www.bloomberg.com/graphics/2016-us-vs-china-economy/

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*: PublicAffairs.

Shema, M. (2010). *Seven deadliest web application attacks*. Burlington, MA: Syngress Media Inc.

Shih, G. (2014, December 8). Chinese Internet regulator welcomed at Facebook campus., *Reuters*. Retrieved from http://www.reuters.com/article/us-china-facebook-visit-idUSKBN0JM0O820141208.

Shin, H. (2015). The Relationship between the Arab Spring Revolutions and Entrepreneurial Inhibitors, Enablers, and Activity in North Africa. In J. Ofori-Dankwa & K. Ormani-Antwi (Eds.), *Comparative Case Studies on Entrepreneurship in Developed and Developing Countries* (pp. 82-98). Hershey, PA: IGI Global.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*: Oxford University Press.

Skepys, B. (2012). Is There a Human Right to the Internet. *J. Pol. & L., 5*, 15.

Soldatov, A., & Borogan, I. (2013). Russia’s surveillance state. *World Policy Journal, 30*(3), 23-30.

Stewart, S. (2013). Epilogue–From the ‘colour revolutions’ to the ‘Arab spring’: Implications for democracy promotion. In S. Stewart (Ed.), *Democracy Promotion and the 'Colour Revolutions'* (pp. 181). London: Routledge.

Story, L. (2007, September 22). Mattel Official Delivers an Apology in China *New York Times*. Retrieved from http://www.nytimes.com/2007/09/22/business/worldbusiness/22toys.html?_r=1&oref=slogin

Stuenkel, O. (2013). Rising Powers and the Future of Democracy Promotion: the case of Brazil and India. *Third World Quarterly, 34*(2), 339-355.

Swyngedouw, E. (2000). Authoritarian governance, power, and the politics of rescaling. *Environment and Planning D, 18*(1), 63-76.

Tan, J., & Tan, A. E. (2012). Business under threat, technology under attack, ethics under fire: The experience of Google in China. *Journal of Business Ethics, 110*(4), 469-479.

Tilly, C., & Ardant, G. (1975). *The formation of national states in Western Europe* (Vol. 8): Princeton Univ Pr.

Trickey, H. (1988). C++ versus Lisp: a case study. *ACM Sigplan Notices, 23*(2), 9-18.

Tully, S. (2014). A Human Right to Access the Internet? Problems and Prospects. *Human Rights Law Review*, ngu011.

Weede, E. (2015). Future Hegemonic Rivalry Between China and the West? *Journal of World-Systems Research, 1*(1), 639-658.

West, D. M. (2016). Internet shutdowns cost countries $2.4 billion last year Washington DC: Brookings Institution Center for Technology Innovation.

Wexelblat, R. L. (2014). *History of programming languages*: Academic Press.

Whiting, A. S. (1996). The PLA and China′ s Threat Perceptions. *The China Quarterly, 146*, 596-615.

Wrobel, D. M. (2013). *Global West, American Frontier: Travel, Empire, and Exceptionalism from Manifest Destiny to the Great Depression*: UNM Press.

Xu, X., Mao, Z. M., & Halderman, J. A. (2011, May 20-21). *Internet censorship in China: Where does the filtering occur?* Paper presented at the 12th Passive and Active Measurement Conference, Atlanta, GA.

Yong, W., & Pauly, L. (2013). Chinese IPE debates on (American) hegemony. *Review of International Political Economy, 20*(6), 1165-1188.

Zhao, S. (2015). Rethinking the Chinese World Order: the imperial cycle and the rise of China. *Journal of contemporary China, 24*(96), 961-982.

Zheng, Y., & Lye, L. F. (2015). China's Foreign Policy: The Unveiling of President Xi Jinping's Grand Strategy. *East Asian Policy, 7*(01), 62-82.