Uncivil and Post-Western Cyber Westphalia: Changing interstate power relations of the cybered age

Dr. Chris C. Demchak

ABSTRACT

Cyberspace is becoming bordered and moving away from westernized civil society control. Governments and major organizations are building a "Cyber Westphalia" of bordered national jurisdictions, forming in pieces across nations. Furthermore, the world has entered into the era of 'cybered conflict' among states and non-state organizations. As the centers of economic and demographic power move to Asia, rising non-westernized states are contesting the western notions of an unbordered, civil society led global cyberspace directly, as well as inevitably western control of the rest of the international economic system. That the challenge happened in less than a generation is, in large part, due to these western societies whose key actors were captured by a tri-part convergence during the formative 'frontier era' of cyberspace. Three cognitive frames guided western approaches to the growing global substrate: unrealistic optimism in early utopian cyber visions, security-blind IT capital goods business models, and western societies' deeply institutionalized hubris about the permanency and moral superiority of their Cold War legacy control of the international system. Time is running out for scholars and practitioners to consider, debate, and consense on alternatives that can rescue 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.

> "Taking away developing countries' ability to control public opinion through Internet controls and surveillance would result not in more openness, but instead in *blood* and *hatred*."
>
> September speech by Hao YeLi, Vice Chair, China Institute for Innovation Development Strategy, former senior officer PLA General Staff. (Mozur 2015)

With engineering, economics, and comparative complex organization theory/political science degrees, Dr. Chris C. Demchak is the RDML Grace M. Hopper Professor of Cyber Security and Director, Center for Cyber Conflict Studies (C3S), U.S. Naval War College. In her research on cyberspace as a globally shared insecure complex 'substrate', Demchak takes a systemic approach to emergent structures, comparative institutional evolution, adversaries' use of systemic cybered tools, virtual worlds/gaming for operationalized organizational learning, and designing systemic resilience against imposed surprise. Recent works include *Designing Resilience* (2010, co-edited); *Wars of Disruption and Resilience* (2011); and a draft manuscript entitled *Cyber Westphalia: Cyberspace's Redefining International Economics, Conflict, and Global Structures.*

Rising Cyber Westphalia

Today, the early halcyon 'frontier era' of cyberspace is over, and its visions have failed. It is not, as the early cyber prophets envisioned—an automatically benign global 'village' open to all, free or nearly free of cost or technological restrictions or borders or governments, uniformly positive in its effects, and automatically democratizing for any citizen or nation that used it. (Rheingold 1993) Cyberspace is becoming bordered and moving away from westernized civil society control.

Over the past twenty-five years of cyberspace's formative 'frontier era', global digitization created a worldwide socio-technical economic system (STES)[1] that serves now as a key substrate underlying and connecting the key functions of all digitizing societies. It did not, however, convert political systems or cultural preferences to the civil society ideals embedded deeply in western democratic government, commercial, and civil society approaches to the global internet. [2] Rather than a universally equitable and unfettered prosperity and democracy spreading globally, the open internet imposed on western nations unprecedented econnomic losses as cyber-enabled criminal transnational organizations (TNOs) and free riders exploited the open, poorly secured global networks. (PWC 2014) Furthermore governments, their proxies, witting fellow travelers, and criminal or activist opportunists adopted global cybercrime's exploit tools and demonstrated techniques to compete with, spy on, disrupt, undermine, and over time debilitate their perceived adversaries. (Riley and Vance 2011)

Instead of the nirvana of no governments and free prosperity, governments and major organizations are building cyber defenses, a "Cyber Westphalia" [3] of bordered national jurisdictions is forming in pieces across nations. As this formative era ends, the world has entered into the era of 'cybered conflict'[4] among states and non-state organizations. As the centers of economic and demographic power are moving to Asia, rising non-westernized states are not simply quietly folding into the existing liberal economic international system as presumed. Rather, led by China in particular, they are less and less likely to 'blindly ape' democratic civil society rules of law. (Peerenboom 2006) They are contesting the western notions of an unbordered, civil society led global cyberspace directly, as well as the inevitability of western control of the rest of the international economic system. (Chen 2001) The rise of these cyber borders coupled with cybered conflict and a growing non-western rejection of western civil society values dramatically reduces the chances that the coming international economic system of the cybered world will reflect the future envisioned by the western democracies who created cyberspace.

Why did western societies lose purchase on the key early formative period of the emerging global structure and the likely imperatives of the future deeply cyber world? While not successful in practice, the early cyber-prophet visions did nonetheless succeed in deeply defining the basic "deep institution"[5] presumptions that framed twenty years of policy objectives in the western democratic civil society's public and private organizations. While declining in their overt expression, the effects of their cognitive framing continue to symbolically and practically distract the key westernized communities from recognizing quite different trends across the international system.[6] Eventually the global system would have altered as a rising China and the other ninety percent of the world's population outside of Europe, the US and their democratic allies modernized. (Nye Jr 2011) However, without cyberspace's open connectivity to both legal and illegal sources of wealth and power-enhancing knowledge, this sea change might have been more gradual, taking three or four generations to truly challenge existing presumptions. Western societies' complacency, however, helped this challenge emerge so quickly by not reacting to accept some—and redirect other—trends as the cyberspace substrate changed underlying interactions and perceptions of interest.

Cyberspace is becoming bordered and moving away from westernized civil society control.

This article argues that three cognitive blinders in western approaches operated over this formative era to hinder accurate assessments of emerging reality: unrealistic optimism in early utopian cyber visions, security-blind IT capital goods business models, and western societies' deeply institutionalized hubris about the permanency and moral superiority of their Cold War legacy control of the international system. The 'winners' of the Cold War ignored the reality of their own cultural uniqueness, of the lack of security concerns for national wealth in their own IT capital goods manufacturing, and of the possibility that the international system created in the Cold War could ever be contested and bested by rising adversaries. A different future is emerging—a crisis-ridden, conflictual, uncivil and post-western Cyber Westphalia.

Optimistic Visions and Naively Insecure Designs

The original internet's design, its optimistic visions, its globalized access to national riches, and its civil society norms are products of the dominance of the civil societies such as the US during the Cold War. Civil society control over the globe's rules of exchange was never inevitable, not permanent, but it was seen as both by the West's policy makers, strategic thinkers, and most academics. Improperly understood was the uniqueness of the first 40 years since the end of World War II, during which time the major peer adversaries—China and Russia—helpfully self-isolated economically. That absence made it possible for the US without too much bloodshed or costs to install and maintain the West's preferences across the international system. [7]

By the middle of the 1990s, after forty years, that system did look to be permanent as former outside states such as Russia and China seemed to be complying more or less. For those creating the visions of the early internet, it was easy to assume nothing else would happen when a communication tool built for western cultural norms and legal enforcement regimes spread to considerably different communications, values, and political systems. (Goldsmith and Wu 2006) Since WWII, other cultures complied; they did not contest—at least not successfully. The technical designers of the original internet were focused on the intellectual challenge of networks and the reliability of transmission—not on security or other cultures. The libertarian commercial entrepreneurs creating the early IT capital goods industry focused on the domestic first before moving to the international markets—assuming both were legally assured by the apparent permanence of the western liberal international economic system. (Feldmann 2010)

Enduring Optimism and Presumptions

After almost three decades of development by US government financial support to universities, cyberspace emerged for public and commercial use about twenty-five years ago as the 'internet'. (Hafner 1999) It was already embedded with the ideology of a public good. Sharing the technological developments and access openly across universities, it became a social presumption embedded as an intrinsic and inevitable requirement for the generation of new ideas, languages, and software. Security was an afterthought, in large part because 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. [8] Furthermore, concerns were limited because early cyberspace did not uniformly connect everything important, and the biggest threats were unreliable transmission, some cybercrime, and possibly sociopathic organizing. (Rochlin 1997) The bigger concern was just getting the sharing to be reliably transmitted. (Kinnersley 2015).

> Over the past 25 years of cyberspace's formative 'frontier era', global digitization created a worldwide socio-technical economic system.

By the mid-1990s, as the internet spread with this presumption of free sharing and access, the new 'cyberspace' acquired almost mystical properties—despite it being completely a man -made, -owned, -maintained, -updated, -monitored, and deployed 'peer-or-pay' underlying sustrate.[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) Otherwise-credible scholars said it would produce a world in which laws emerge from the collective consciousness without governments or national boundaries. That vision 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 global space for good, uplifting all who connected into it.[10] (Norris and Jones 1998)

Commercialization of Flawed Basic Design for Speedy Marketing

Converging with this vision of a new free world of ideas and collective virtual freedom was an oversized set of promises about economic prosperity from the e-commerce and IT capital goods industries. The utopian vision merged with the libertarian view that the Internet and all of its technological designs and development were something that 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.[11]

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) By the early 1990s, the demand from the private sector to 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. (Frischmann 2001) From then on, the influence of commercialization on the dominant design of the web was profound. Those more secure academic languages which took too long and too many resources for commercial returns were displaced.[12] (Trickey 1988) Funding flowed to those computer scientists migrating from the earlier languages known to be intolerant of mistakes in code, such as the LISP (1960s on), 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 a healthy return on his software investment. 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[13] of standardized, fault-tolerant (more easily hacked) software getting to the market as quickly as possible.[14] (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)

So dominant was this perception of the libertarian IT capital goods business model as benign and uniformly economically advancing that it migrated into the taken-for-granted presumptions of the cyber utopian communities as well. With both communities coming to view the open internet's economic benefits as explicitly tied to a lack of government controls for any reason, these communities came to view erecting national jurisdictions across cyberspace as economically daft as well as morally unacceptable in this new cybered world.[15] (Lessig 2004/original 1998) 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.[16] (Betz and Stevens 2011)

Predation at Global Scale Prompts a National Searches for Bolt-On or Keep-Out Options

Rather than democracy and ubiquitous prosperity, the rapidly coded, more easily hacked languages which dominated exchange and hardware across the open, insecure cyberspace enabled the rise of transnational predators en masse. This now freely available, insecure, global substrate offered small and large bad actors three major nearly free advantages never available in history to anyone other than emperors or superpowers—open access to large scale in organizations, to globally close proximity, and to unprecedented levels of precision in remote operations.[17] A massive underground global cybercrime market developed with specialized submarkets, warranties, and tools including services. (Glenny 2011) Governments and transnational criminal organizations soon joined into the global hacking for information, money, and political or economic leverage.[18] A dizzying variety of predators and adversaries for a wide range of reasons—including 'because we can'—now 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.[19]

Even what was once the remaining superpower—the United States—found it did 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, 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. According to a recent 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)

The utopian vision merged with the libertarian view that the Internet and all of its technological designs and development were something that governments and borders should never touch.

Cyber Westphalia Rising Unwitting in the West and Eagerly in the East

Borders rise for many reasons, but largely for reasons of security—i.e., increasing certainty about averting losses from nature or adversaries.[22] As the cyber extractions from victim nations have mounted dramatically, so have the cyber defenses in bits and pieces across nations. (Deibert and Crete-Nishihata 2012) The great threats to economic vitality and nationally critical infrastructure via cyberspace now offer adversaries the potential to cripple the modern state over time while avoiding traditional kinetic war. While the foreign policy language still strongly endorses and calls for a globally free and open internet, the domestic policy language of concern by westernized government has risen from cybercrime, to critical infrastructure protection, and to losses to the entire economy over time, with cyber security now labeled a tier 1 threat.[23] Even nations known for their civil society, Sweden for example, have taken steps domestically to monitor[24] what enters or leaves their national territories networks. The intent is security—to use that information if needed to protect citizens, enforce the laws, or ensure the nation's critical functions.[25]

Yet the symbolic visions of the cyber libertarian and the commercial power of the IT capital goods communities continue to dominate in collective opposition to legitimizing national borders in cyberspace. (Kroker and Kroker 1996) This rejection endures for a third and most embedded reason—the deeply institutionalized western sense that democracy is the inevitable end state of all societies. (Wrobel 2013) Borders in the internet are unnecessary and immoral—as well as generally wastefully futile—impediments to achieving that global end state. (Atkinson and Brake 2015)

China's Sovereignty Narrative and Western Hubris

> "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)

China wants her borders in cyberspace and will take nothing less. (Gresh 2008) Yet an unacknowledged western hubris—a supreme confidence in the moral and economic superiority of the western approach to society and cyberspace, however, leads governments and civil society promoters to consistently refuse to accommodate the Chinese sovereignty demand. They routinely conflate civil society cyber societies with economic success, despite China's rise having already demonstrated to the rest of the world that the two could be separated successfully.[26] (Kalathil and Boas 2010) Furthermore, China is not alone. The Chinese model of societal information control and their wider neo-capitalist business practice preferences have a powerful resonance with the rest of the non-westernized world. (Chen 2001)

Since entering the global web in the 1990s, China's spokespersons have consistently made its sovereignty expectation explicit—including across the internet. (Whiting 1996) China's leaders had relatively good reasons to expect a campaign to alter the global narrative to accept simply national sovereignty in cyberspace would be successful. (Qiu 1999) 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.[27] (Yong and Pauly 2013) Given the Cold War history, the leaders of China, Russia, and many other non-westernized leader could 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.[28] (Blum 2013) Furthermore, the United Nations is a foundation of the post-WWII liberal international system and its basic multilateral character has been reinforced by the international system's decisions strictly upholding sovereignty, even while led by the United States. China's strategists may be forgiven for not recognizing what they faced in the opposition. If one was not taken with the optimism visions, swayed by the economic libertarianism, or imbued with a western superiority hubris, expecting sovereignty would be more or less automatic is a reasonable opening position.

By 2011, China's leaders had taken a decade to position themselves and some allies in key influential positions in international technical organizations, and across critical IT and related markets. However, achieving an endorsement of cyber sovereignty by the international community did not emerge. Rather, 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.[29] Furthermore, the civil society promoters have moved the terms of the debate in order to build another obstacle to acknowledging the primacy of national cyber sovereignty. Internet governance conferences—not sponsored by China, close allies, or the UN—now elevate the moral and efficacy value of 'multistakeholder' 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]

In the last four years, Chinese senior political and corporate leaders have moved to an even more aggressive use of rising economic power[31] with an openly wider agenda. The new wider narrative uses the rise of China as a future great or super power to rationalize its right to question the current international system's governors. (Li and Shaw 2014) Not only is China determined to ensure its own national sovereignty in cyberspace and in other sectors, but also they now overtly challenge the western dominance of global Internet governance system as a whole. The apparent objectiveis to influence changes in cyberspace producing a structure more convenient, or at least less threatening, to Chinese national preferences (DeNardis 2014) 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. (Liu and Deng 2010) With its poorly secured global pathways across poor and wealthy national socio-technical-economic systems, cyberspace shortened that transition dramatically—to fifteen to twenty years. (Drezner 2004) China's public and commercial leaders and thinkers now see an opportunity to advance more quickly and are moving to seize the opening.

Even nations known for their civil society—Sweden for example—have taken steps domestically to monitor what enters or leaves their national territories' networks.

Moving to alter cyberspace's international realities has proven illuminating for China.

For example, its meteoric economic rise may have been funded in good part by its cyber business knowledge and data extractions; however, 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) The unclassified 2013 Mandiant report empirically leaves little doubt that an aggressive Chinese military unit (among others) has been one key source of the massive cyber data extractions. (Mandiant 2013) Yet very little punitive action has been publicly announced in international fora, in markets, or bilaterally as corrections on China for these activities emanating from its territory. In 2000, China was allowed to enter the World Trade Organization (WTO) due to its size and despite its inability to meet the basic WTO obligations. (Blancher and Rumbaugh 2004) By 2014, however these requirements have never been met, and yet there is no discussion of ejecting China. (Atkinson and Ezell 2015) Rather, by 2015 the US President and China's President Xi signed an agreement on cybercrime and data extractions that has no mechanisms for enforcement. (Hvistendahl 2015) This level of agreement, and the general tolerance of poor behavior internationally, constitute the kind of accommodations made between peer great powers, an inference that Chinese media has noted. (Hao 2015)[32] Indeed, despite signing the 2015 agreement to curb cybered exploitations of information for commercial benefit, the evidence is that Chinese hackers continued at the same pace during and after the fall signing, although the composition of the 'usual suspects' changed.[33]

Furthermore, while China's narrative on cyber borders seems to fall on deaf ears in western states' foreign policy circles, by 2015 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.[34] 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. (Rowley 2010; Liu and Deng 2010) From the practical perspective of developing nations' leaders for whom the Chinese firm Huawei is building—for the national telecommunications public agency—4G networks for nearly no upfront costs, opposing borders in cyberspace conflicts with the rising reality. (Gagliardone 2015) (Chung and Mascitelli 2014)

Building on the opening provided in its fight for national cyber sovereignty, China now routinely uses its own version of 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 explicit western expectation that cyberspace under civil society will democratize a society, the Chinese narrative accentuates the instability and greater dissent that can accrue with a border-spanning open internet. (Cui and Wu 2016) This dissent can prove unhealthy for authoritarian or semi-governed states and their leaders, and the 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) Left open is how this fully bordered cyberspace is to be governed internationally. However, the Chinese narrative in speeches and publications then connects this essential element, state cyber sovereignty, with a world where China rises to its proper place as the first great power that is benignly 'non-hegemonic'. The term is used to mean no state including China as a rising world power will tell any other state how to operate internally, thus neatly eliminating the US as the old style global internet hegemon with its civil society preferences from the center of the global international system's governance. (Kivimäki 2014)

China has moved fast from its frustrations with the West on cyber sovereignty to more aggressively seizing on the international influence openings offered by a hegemon and allies apparently unable or unwilling to bribe or bully China and allies into compliance. While not eager for military confrontation, conflicts with the US on economic, information, institutional, and cultural fronts have been expected by China's pragmatists for some time, seen as an inevitable outcome when a current hegemon resists being displaced. (Liu 2015) (Zhao 2015) 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 web dominance. (Kemp 2015) The Chinese narrative has hardened publicly against the combination of cyber utopian vision, libertarian economics, and westernized civil society hubris. (Zheng and Lye 2015). While much in cyberspace is classified in western nations, the battlefield for this narrative is not. In response, many internet governance-related forums: GFCE, IGF, Global Commission on Internet Governance, NETmundial Initiative, WSIS, WCIT, and the GCCS 'London Process' have signaled a redoubling rather than weakening of western pressure for China's acquiescence to UN human rights applied to cyberspace internally as part of the future cybered world system.[35] Tensions are deepening across cyberspace.

By 2015, President Obama and China's President Xi signed an agreement on cybercrime and data extractions that has no mechanisms for enforcement.

Cybered Conflict and Rising Post-western Cyber Westphalia

Not only has the West lost purchase on whether national borders (re:jurisdictions) are erected in cyberspace, its three collective cognitive failures: vision, business model, and hubris have also encouraged the conditions for cybered conflict as these borders rise. With the western actors increasingly accusing China of a myriad of cybercrime and other violations of civil society laws and expectations, China's response is to deny accusations, and accuse in return. China also uses the full weight of its demographic and economic power, by fair means and foul [36] across a range of overt and covert activities, to change the perceptions of potential allies about their own economic and societal interests versus supporting US cast as the failed hegemon of the internet. (Karatzogianni 2010) With the two major nations at loggerheads over governance and pride of first place, the Cyber Westphalian system rises around them; highly conflictual in cybered terms, and possibly also in kinetic terms on occasion.

Cybered conflict is two, or more, faced. While its lack of overt violence encourages system versus system conflict to remain generally short of traditional kinetic war, the deceptiveness in tools and opaqueness of originators inherent to its operations undermine existing conflict-dampening institutions, tropes, and norms. (Goldsmith 2013) On one hand, China's cyber forces, volunteers, and proxies can do a great deal to make it harder for westernized actors to persuade, bribe, or bully enough other states to truly consolidate enforceable international rules against sovereignty or ensure democratic human rights. In a deeply cybered world, options abound from cybered conflict's three advantages in scale, proximity, and precision for conducting long running, below physical conflict, global campaign through social media, [37] largescale economic extractions, and increasingly sophisticated international mercantilism. (USCESRC 2014) (Perlroth 2013) Also available are multiple avenues by which to individually bride or bully, including blackmail or intimidation, others in major or allied nations' positions to work against the West's role and its allied unity across a wide variety of international venues, especially those dealing with global governance of cyberspace. (Shakarian et al. 2013)

On the other hand, cybered conflict's mechanisms and tools are largely developed by the international cybercrime community not under any state's credible control as yet. Furthermore, these criminals' excesses, many from China, are what majorly drives the westernized states to build national borders unwillingly or unwillingly despite the foreign-policy positions. The massive economic losses have alerted the western security and political leaders to the kinds of behaviors associated with cybercrime, cybered conflict, and even China itself. This economic loss recognition has crystallized a public divide between China with its pro-sovereignty allies, and the western consolidated democracies. (Lindsay 2013) For example, the US and its allies walked out of a heavily pro-sovereignty 2012 WCIT meeting hosted by the UN's ITU, which is increasingly influenced by China, recognizing they were going to lose a major vote. (Huston 2012) That collective demonstration of strong displeasure is unusual for western states. However, when such behavior is conducted by those who thought their preferences ruled the international system, it suggests strongly that the changes China hopes to see may not be quietly accepted. (Jardine et al. 2015)

Cybered conflict also encourages misperceptions particularly due to the wide variation in the number of state and nonstate actors, and events that could be engaged at any given moment. Just as the West has continually got it wrong and set up the conditions for this conflict so rapidly, so too can China misperceive how far is risky in pushing for more than simply cyber sovereignty. While the US sees its efforts as benignly trying to help a peaceful rise of China into democracy, the Chinese elites view the western anti-border and civil society efforts as either inexplicably stupid, or an indication of a larger more threatening plan. (Gardner 2015) As they act and western security institutions respond, a wide variety of connected critical systems are being employed in this contest across cybered nations and complex systems. The greater the number of actors involved, the more surprise and misjudgment are encouraged. The two main adversaries routinely misperceive each other. The US sees itself as simply defending a universal good in an open global Internet by still rejecting borders and calling for universal civil society values. On the other hand, a cyber-emboldened China presents itself is merely trying to be sovereign as it develops. It is also hoping to hurry along the hegemon's apparent decline with narratives, money, and stealth, and yet control the narrative of a no-threat peaceful rise well enough to stay short of physical conflict. Across a global and highly insecure underlying substrate, however, a plethora of other actors and systems actively, unwittingly, or unwillingly also have multiple options at low cost to enter the struggle and muddle the indicators and conditions that both the US and China perceive. In pursuing what seems a golden opening to shorten the path to the global top rank, China's leaders and their allies could easily misjudge the level of quiescence the western powers will exhibit as their utopian, libertarian, and hubris-borne presumptions fail to deliver.

> The massive economic losses have alerted the western security and political leaders to the kinds of behaviors associated with cyber-crime, cybered conflict, and even China itself.

As trends stand today, the deeply interconnected mass of national socio-technical economic systems will increasingly reflect the preferences of more authoritarian states in the emergent center of economic power in Asia. (Berger 2015) Chinese business practices, in particular, are personalistic, social clan based, affective, opaque, and quite variant from the western economic world of legal protections and transparent, enforced contracts. (McDonald 2012) Without a compensating balance in economic and political weight by the small number of states that are consolidated democratic civil societies, such things as common liberal technological standards, transparency in currency stability, and open, nonarbitrary rule of law support for international commercial contracts and IP will slowly migrate to reflect the routinely nontransparent Asian—specifically Chinese—business as preferences, along with internet governance structures. (Bu and Roy 2015) (Hannas et al. 2013)

China's thinkers increasingly discuss how the West, specifically the US, might respond as the failing hegemon, and, to be fair, some form of this cybered competition between the US and China would have emerged anyway. However, without the distraction of a vision, the economic libertarian push, and the border and values insults energizing a rising adversary, cybered conflict is likely to have emerged more slowly with differently weighted advantages. The delay would have better encouraged western democratic public and commercial leaders to recognize the negative global trends and to find more studied, grounded, and feasible paths in adapting to differing global power distributions. China's leaders would still have believed that their population weight in the world entitles their rise to be one of two great powers in the world at some point in the future. Cyberspace's vulnerabilities would still have made hacking for profit into opportunities to level the playing field in securing China's rise, but these opportunities do not make it urgent to move more quickly. When the current internet hegemon and its allies constantly seem to threaten the fundamentals of China's political system, then it does become less tolerable for China to wait until the 2049 date (or later) anticipated by Deng Xiaoping for this rise of China to be settled. Still, China might have moved more circumspectly, had the discovery of the massive losses in economic wealth produced firm reactions by the West—ones that would be more likely to be interpreted in China as worthy of a strong hegemon. In recent years, China strategic and economic actors have overcome their surprise at how little the West, specifically the US, has done publicly about the economic violations, other then repeated calls for civil society norms and meetings. Many Chinese publications now openly assume the apparently quite rapid decline of the US as a hegemon as mere segue to addressing the urgent need for China to take the opportunity to accelerate its rise.[38]

> The US sees itself as simply defending a universal good in an open global Internet by still rejecting borders and calling for universal civil society values.

This Internet governance challenge to civil society presumptions is only the beginning of a host of looming multi-domain contests more likely to be lost in the future if the West is unable to recognize and alter the cognitive framing created in the early frontier era of cyberspace. It has been costly for the western democracies to be so distracted. 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. Even if western national leaders abruptly announced acceptance of a global system of national cyber sovereignties, the civil society narrative now has a major, well-funded, covertly reinforced, and overtly well promoted counter-narrative about the rules governing the future cybered world led by more authoritarian sensibilities. To be blunt, there are no guarantees of dominance—or even a future world filled with democracies—for the consolidated democratic civil societies who are less than ten percent of the globe's population.[39] In any era, it is tough to cement allies if one is seen to be in decline. In the near to far term, there is no clear path by which these western economies could support the level of Cold War enforcement efforts ensuring the world would follow their lead.

The liberal international economic system cannot survive long on its own, save possibly in name only without its wealthy western civil society governors and enforcers. Nonwestern cultures indifferent to civil society values were not offered much of a middle ground in the western vision of the global cyberspace, not even the option to be sovereign within their own networks. Now China and Russia, among others, offer that sovereignty as a minimum in their alternate narrative, along with political models that can seem more likely to be stable internally than democracy, and yet, economically advancing.[40] Indeed, Ringmar (2012) offers the proposition that given differences in power sources, use of emotions in foreign policymaking, and the over reliance on the vagaries of socially mediated public opinion formation, the two quite different international systems in history (Sino-centric or the Tokugawa Japan) may prove better adapted than the Westphalian system to the kinds of conflict and social organizing needed in the coming deeply cybered and conflictual century. (Ringmar 2012) This notion may be extraordinarily offensive to those imbued with the dominant triumphalism of western democracies, but not to the other ninety percent of the globe's population likely to be led by the practices, preferences, and products of China and Asia for most of the rest of this century.

Forcing the future global cyberspace to keep to the western model of an open internet transiting into and across all nations is normatively desirable, but it is no longer possible. Needed urgently is a feasible alternative structure for a conflictual cybered world—one that is markedly less than global, less than normatively preferred, and less consumed with globalizing western libertarian economics. 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. This honest conversation and critical research about the future of the international socio-technical-economic system needs to begin now.[41] The alternative is to eventually concede to a global version of China's 'info-web' internet. (Schneider 2015) The conflictual and eventually post-western cyber Westphalian international system is rising very fast indeed.

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

BIBLIOGRAPHY

Anderson, Ross J. 1994. “Liability and computer security: Nine principles.” *In Computer Security—ESORICS 94:* Springer.

Atkinson, Robert, and Doug Brake. 2015. “Net Gains: A Pro-Growth Digital Agenda.” *Democracy* (36):9.

Atkinson, Robert D., and Stephen Ezell. 2015. “False Promises: The Yawning Gap Between China’s WTO Commitments and Practices.” Washington DC: Information Technology and Innovation Foundation.

Barlow, JP. 1996. “A Declaration of the Independence of Cyberspace.” *Humanist - Buffalo 56* (3):18-9.

Barrett, Louise, S Peter Henzi, and David Lusseau. 2012. “Taking sociality seriously: the structure of multi-dimensional social networks as a source of information for individuals.” *Philosophical Transactions of the Royal Society of London B: Biological Sciences 367* (1599):2108-18.

Barry, Jack Joseph. 2014. Don't Be Evil: Should Access to the Internet Be Conceptualized as an Instrumental Human Right? Paper read at American Political Science Association 2014 Annual Meeting Paper.

Berger, Ron. 2015. “The transformation of Chinese business ethics in line with its emergence as a global economic leader.” *Journal of Chinese Economic and Foreign Trade Studies 8* (2):106-22.

Betz, David J, and Tim Stevens. 2011. “Chapter two: Cyberspace and sovereignty.” *Adelphi Series 51* (424):55-74.

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

Blanchard, Jean-Marc F, and Norrin M Ripsman. 2008. “A political theory of economic statecraft.” *Foreign Policy Analysis 4* (4):371-98.

Blancher, Mr Nicolas R, and Mr Thomas Rumbaugh. 2004. “IMF: China - international trade and WTO accession.” International Monetary Fund.

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

Blumler, Jay G, and Stephen Coleman. 2001. *Realising democracy online: A civic commons in cyberspace.* Vol. 2: IPPR London.

Bradley, James. 2015. The China Mirage. New York: Little, Brown and Company.

Brink, Gustav Francois. 2013. “Anti-dumping and China: three major Chinese victories in dispute resolution.”

Bu, Nailin, and Jean-Paul Roy. 2015. “Guanxi Practice and Quality: A Comparative Analysis of Chinese Managers’ Business-to-Business and Business-to-Government Ties.” *Management and Organization Review 11* (02):263-87.

Cerf, Vinton G. 2012. “Internet access is not a human right.” New York Times 4:25-6.

Chen, Ming-Jer. 2001. *Inside Chinese business: A guide for managers worldwide.* Cambridge, MA: Harvard Business Press.

Chung, Mona, and Bruno Mascitelli. 2014. “Huawei’s Battle: Cold War or Commercial War?” *Asian Business and Management Practices: Trends and Global Considerations: Trends and Global Considerations:107.*

Clark, David. 2010. “Fighting over the Future of the Internet.” IEEE Internet Computing 10:22-3.

Cui, Di, and Fang Wu. 2016. “Moral goodness and social orderliness: An analysis of the official media discourse about Internet governance in China.” *Telecommunications Policy 40* (2-3):265-76.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace:* McClelland & Stewart.

Deibert, Ronald J, and Masashi Crete-Nishihata. 2012. “Global governance and the spread of cyberspace controls.” *Global Governance: A Review of Multilateralism and International Organizations 18* (3):339-61.

Demchak, Chris C. 2012. “Resilience, Disruption, and a ‘Cyber Westphalia’: Options for National Security in a Cybered Conflict World.” In *Securing Cyberspace: A New Domain for National Security,* ed. N. B. a. J. Price. Washington, DC: The Aspen Institute.

BIBLIOGRAPHY

———. 2013. "Economic and Political Coercion and a Rising Cyber Westphalia." In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,* ed. K. Ziolkowski. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Demchak, Chris C., and Peter J. Dombrowski. 2011. "Rise of a Cybered Westphalian Age" *Strategic Studies Quarterly 5* (1):31-62.

DeNardis, Laura. 2014. *The global war for internet governance:* Yale University Press.

Diamond, Larry Jay. 1994. "Toward democratic consolidation." *Journal of Democracy* 5 (3):4-17.

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

Duara, Prasenjit. 1997. "Transnationalism and the predicament of sovereignty: China, 1900-1945." *The American Historical Review:*1030-51.

Dunlap Jr, Charles J. 2001. "Law and military interventions: preserving humanitarian values in 21st century conflicts." In *Humanitarian Challenges in Military Intervention Conference,* ed. K. S. o. G. Carr Center for Human Rights Policy, Harvard University. Washington, DC.

Farnsworth, Timothy. 2011. "China and Russia Submit Cyber Proposal ["International code of conduct for information security"]." *Arms Control Today:*35-6.

Feldmann, Anja. 2010. *The Internet Architecture-Is a Redesign Needed?:* Springer.

Fountain, J. E. 2001. *Building the Virtual State: Information Technology and Institutional Change:* Brookings Institution Press.

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

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

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

Gardner, Maggie. 2015. "Channeling Unilateralism." *Harv. Int'l LJ* 56:297.

Glenny, Misha. 2011. *Dark Market.* New York: Random House.

Goldman, David. 2011. "The cost of cybercrime—The price tag on corporate data breaches is soaring: The rise in cyber-crime is costing hundreds of billions of dollars each year." *CNNMoney.com,* July 22.

Goldsmith, Jack. 2013. "How cyber changes the laws of war." *European Journal of International Law* 24 (1):129-38.

Goldsmith, Jack L, and Tim Wu. 2006. *Who controls the Internet?: illusions of a borderless world.* Vol. 89: Oxford University Press New York.

Goodin, Dan. 2010. "IE zero-day used in Chinese cyber assault on 34 firms: Operation Aurora unveiled." *El Register,* January 14.

Gorman, Siobhan. 2012. "Chinese hackers suspected in long-term Nortel breach." *The Wall Street Journal,* February 14.

Grant, Tim. 2014. On the Military Geography of Cyberspace. Paper read at ICCWS2014-9th International Conference on Cyber Warfare & Security: ICCWS 2014.

Greer, John 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* 4:139-54.

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

BIBLIOGRAPHY

Hannas, William C, James Mulvenon, and Anna B Puglisi. 2013. *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation:* Routledge.

Hao, Qi. 2015. "China Debates the 'New Type of Great Power Relations'." *The Chinese Journal of International Politics* 8 (4):349-70.

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

Hughes, Kristin Ashburst. 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.

Huston, Geoff. 2012. "Calling Stumps at WCIT: Win, Lose or Draw?" In *The ISP Column.* http://wattle.rand.apnic.net/ispcol/2012-12/stumps.pdf.

Hvistendahl, Mara. 2015. "Not guilty as charged." *Science* 350 (6262):732-5.

Irion, Kristina. 2009. "Privacy and security International communications surveillance." *Communications of the ACM* 52 (2):26-8.

Jardine, Eric, Samantha Bradshaw, Dr DeNardis, Fen Osler Hampson, and Mark Raymond. 2015. "The Emergence of Contention in Global Internet Governance (Rpt 17)." *In Global Commission on Internet Governance (CIGI).* London: Chatham House.

Juuso, Anna Maija, Ari Takanen, and Kati Kittilä. 2013. Proactive cyber defense: Understanding and testing for advanced persistent threats (APTs). Paper read at Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013.

Kalathil, Shanthi, and Taylor C Boas. 2010. *Open networks, closed regimes*: The impact of the Internet on authoritarian rule. Washington DC: Carnegie Endowment.

Karatzogianni, Athina. 2010. "The Thorny Triangle: Cyber Conflict, Business and the Sino-American relationship in the global system." *e-International Relations.* Online.

Kayaoglu, Turan. 2010. "Westphalian Eurocentrism in international relations theory." *International Studies Review* 12 (2):193-217.

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

Keohane, Robert Owen, and Joseph S Nye. 1977. *Power and interdependence: World politics in transition:* Little, Brown Boston.

Kinnersley, Bill. 2015. "A Chronology of Influential [computer] Languages, The [Computer] Language List: Collected Information On About 2500 Computer Languages, Past and Present." http://people.ku.edu/~nkinners/LangList/Extras/langlist.htm: University of Kansas.

Kivimäki, Timo. 2014. "Soft power and global governance with Chinese characteristics." *The Chinese Journal of International Politics* 7 (4):421-47.

Kopetz, Hermann. 2011. "Internet of things." In *Real-time Systems,* ed. H. Kopetz: Springer.

Kroker, Arthur, and Marilouise Kroker. 1996. "Code Warriors." *CTheory.net:*2-7.

Langheinrich, M. 2001. "Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems." LECTURE NOTES IN COMPUTER SCIENCE:273-91.

Lessig, Lawrence. 2004(1998 original). "The laws of cyberspace." In *Readings in cyberethics,* ed. R. A. Spinello and H. T. Tavani. Sudbury, MA: Jones and Bartlett Learning.

Lewis, James, Lara Crouch, and Anastasia Mark. 2015. "Cybersecurity in Asia and the Role of US Leadership: an Interview with James Lewis." *Georgetown Journal of Asian Affairs* online https://repository.library.georgetown.edu/bitstream/handle/10822/761158/GJAA%202.1%20Lewis,%20James.pdf?sequence=1&isAllowed=y.

BIBLIOGRAPHY

Li, Xing, and Timothy M Shaw. 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.

Lindsay, David F. 2013. "What Do the XXX Disputes Tell Us About Internet Governance? ICANN's Legitimacy Deficit in Context." *Telecommunications Journal of Australia* online 63 (3):http://doi.org/10.7790/tja.v63i3.432 (link is external).

Liu, Jianhua, and Biao Deng. 2010. "America Hegemony: Is It To Decline or To Continue." *Pacific Journal* 1:1-8.

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

Mandiant, APT. 2013. "APT1 Report: Exposing One of China's Cyber Espionage Units (Feb. 2013)". http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

McConnell, Mike, Michael Chertoff, and William Lynn. 2012. "China's Cyber Thievery Is National Policy—And Must Be Challenged." *The Wall Street Journal.*

McDonald, Paul. 2012. "Confucian foundations to leadership: a study of Chinese business leaders across Greater China and South-East Asia." *Asia Pacific Business Review* 18 (4):465-87.

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

Nakashima, Ellen. 2013. "US Target of Massive Cyber-Espionage Campaign." *Washington Post.*

———. 2015. "Following U.S. indictments, China shifts commercial hacking away from military PLA to civilian agency MSS." *Washington Post,* November 30.

Norris, Pippa, and David Jones. 1998. "Virtual democracy." *Harvard International Journal of Press Politics* 3:1-4.

Norton-Taylor, Richard. 2010. "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,* October 18.

Nye Jr, JS. 2011. *The Future of Power in the 21st Century.* Cambridge, MA: Public Affairs.

Oyedemi, Toks. 2014. "Internet access as citizen's right? Citizenship in the digital age." *Citizenship Studies*:1-15.

Paganini, Pierluigi. 2013. "Cyber-espionage: The greatest transfer of wealth in history." *H+ Magazine online,* March 01.

Peerenboom, Randall. 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):192-9.

Perlroth, Nicole. 2013. "Hackers in China attacked The Times for last 4 months." *The New York Times,* January 30.

Philpott, Daniel. 1999. "Westphalia, authority, and international society." Political Studies 47 (3):566-89.

Pillsbury, Michael. 2015. *The hundred-year marathon: China's secret strategy to replace America as the global superpower:* Henry Holt and Company.

Ponemon_Institute. 2012. "Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles." http://www.hp.com/hpinfo/newsroom/press/2012/121008a.html Hewlitt Packard Research.

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

Rheingold, H. 1993. Virtual Communities: Homesteading on the Electronic Frontier. Reading, UK: Addison Wesley.

Richmond, Riva. 2011. "The RSA Hack: How They Did It." *New York Times,* April 2.

Riley, Michael, and Ashlee Vance. 2011. "Cyber Weapons: The New Arms Race (The Pentagon, the IMF, Google, and others have been hacked. It's war out there, and a cyber-weapons industry is exploding to arm the combatants)." *Business Week,* July 20.

BIBLIOGRAPHY

Ringmar, Erik. 2012. “Performing international systems: two East-Asian alternatives to the Westphalian order.” *International Organization* 66 (01):1-25.

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

Rogers, Mike, and Dutch Ruppersberger. 2012. “Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE: A Report.” Washington DC: US House of Representatives.

Rosenzweig, Roy. 1998. “Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet.” *American Historical Review*:1530-52.

Rowley, Chris. 2010. “Commentary: China’s chimera: miracle or mirage in the ‘Middle Kingdom’?” *Asia Pacific Business Review* 16 (3):269-71.

Scheinmann, Gabriel M, and Raphael S Cohen. 2012. “The Myth of “Securing the Commons”. *The Washington Quarterly* 35 (1):115-28.

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

Schrage, Michael. 2011. “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* online.

Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. 2013. “The Dragon and the Computer: Why Intellectual Property Theft is Compatible with Chinese Cyber-Warfare Doctrine.” In *Introduction to Cyber-Warfare: A Multidisciplinary Approach* ed. P. Shakarian, J. Shakarian and A. Ruef. New York: Syngres.

Shih, Gerry. 2014. “Chinese Internet regulator welcomed at Facebook campus.” *Reuters,* December 8.

Shin, Henry. 2015. “The Relationship between the Arab Spring Revolutions and Entrepreneurial Inhibitors, Enablers, and Activity in North Africa.” In *Comparative Case Studies on Entrepreneurship in Developed and Developing Countries,* ed. J. Ofori-Dankwa and K. Ormani-Antwi. Hershey, PA: IGI Global.

Singer, Peter W, and Allan Friedman. 2014. *Cybersecurity: What Everyone Needs to Know*: Oxford University Press.

Stewart, Susan. 2013. “Epilogue–From the ‘colour revolutions’ to the ‘Arab spring’: Implications for democracy promotion." In *Democracy Promotion and the* ‘*Colour Revolutions*’, ed. S. Stewart. London: Routledge.

Story, Louise. 2007. “Mattel Official Delivers an Apology in China” *New York Times,* September 22.

Stuenkel, Oliver. 2013. “Rising Powers and the Future of Democracy Promotion: the case of Brazil and India.” *Third World Quarterly* 34 (2):339-55.

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

Tully, Stephen. 2014. “A Human Right to Access the Internet? Problems and Prospects.” *Human Rights Law Review*:ngu011.

USCESRC. 2014. “2014 Annual Report to the US Congress.” In *Annual Reports to the US Congress,* ed. U.-C. E. S. Commission. http://www.uscc.gov/Annual_Reports/2014-annual-report-congress.

Wexelblat, Richard L. 2014. History of programming languages: *Academic Press.*

Whiting, Allen S. 1996. “The PLA and China’s Threat Perceptions.” *The China Quarterly* 146:596-615.

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

Xu, Xueyang, Z Morley Mao, and J Alex Halderman. 2011. Internet censorship in China: Where does the filtering occur? Paper read at 12th Passive and Active Measurement Conference, May 20-21, at Atlanta, GA.

Yong, Wang, and Louis Pauly. 2013. “Chinese IPE debates on (American) hegemony.” *Review of International Political Economy* 20 (6):1165-88.

Zhao, Suisheng. 2015. “Rethinking the Chinese World Order: the imperial cycle and the rise of China.” *Journal of contemporary China* 24 (96):961-82.

Zheng, Yongnian, and Liang Fook Lye. 2015. “China's Foreign Policy: The Unveiling of President Xi Jinping’s Grand Strategy.” *East Asian Policy* 7 (01):62-82.

Zittrain, J. 2006. “A History of Online Gatekeeping.” *Harvard Journal of Law & Technology* 19 (2):253-98.

NOTES

[1] This unprecedented and increasingly critical national-level connectivity and its effects requires expanding the well-established 'socio-technical systems' (STS) concept to reflect 'socio-technical-economic-systems (STES) undergirding the modern digitized society. The newer term is needed to spur a new generation of economic, societal, and interstate conflict theories designed for a cybered world of interpenetrating and conflictual national STESs. (Dombrowski and Demchak 2014)

[2] The US developed a "free flow" doctrine as the basic tenet of US policy-making towards the internet. (Powers and Jablonski 2015) In Europe where it is not contested that commerce is regulated by governments, these ideals emphasized an 'unrestricted access' doctrine wherein citizens are completely free to access to the internet for social communications, as ensured as a moral obligation by governments. http://eeas.europa.eu/policies/eu-cyber-security/.

[3] The "Westphalian" system began with the 1648 Peace of Westphalia treaty by which two neighboring European states agreed to the reciprocal recognition of consensually identified national borders. (Philpott 1999) The current and taken for granted permanency of these borders is profoundly a product of the Cold War era. (Kayaoglu 2010) See also (Demchak and Dombrowski 2011)

[4] 'Cybered conflict' is unique to this emerging era in that it is a spectrum between peace and traditional war in which nations and transnational organizations use the deception in tools, opaqueness in originators with the three low cost offense advantages of scale, proximity, and precision to hinder each other's STESs in part or in whole, waxing and waning, and iterating according the opportunities. Cybered conflict is a newer form of system versus system nonobvious conflict that is uniquely enabled by the insecure design of the global cyberspace. Cyberspace itself is not a 'commons' or increasingly even a 'shared resource' as envisioned by thinkers in the democratic societies.(Blumler and Coleman 2001) (Scheinmann and Cohen 2012) Rather, it is best viewed as a 'substrate' that spread under and penetrated up into every major society's critical functions, linking a wide variety of actors, critical processes, and wealth in unprecedented ways. (Demchak and Dombrowski 2011; Grant 2014) All conflicts of societal significance will be cybered henceforth. Few will be traditionally declared, kinetic, two nation struggles, making the national security tasks of democratic nations in particular much more challenging than any era since WWII. (Dombrowski and Demchak 2014)

[5] Fountain argues that, once these notions become taken for granted as "deep institutions", it is extraordinarily difficult to get their adherents to recognize their binding power, let alone to change those barring highly unsettling events or long-term campaigns to wear down the usefulness of these notions for shared daily practices. (Fountain 2001)

[6] A small but growing number of scholars and practitioners have publicly noted these deeply held presumptions. More recently, James Lewis of CSIS in Washington, a noted expert on cyber international relations, especially between the US and China, has reiterated with some frustration the enduring nature of these wildly optimistic, but rarely openly questioned presumptions. (Lewis et al. 2015) It must also be noted that a small handful of respected scholars supporting a globally open internet are clear-eyed about the true chances of achieving this normatively desirable outcome; they are to be applauded for their courage and persistence, and are not the target of this critique. In particular, works by Rob Deibert and his co-authors associated with the Munk Center, University of Toronto demonstrate this category. (Deibert 2013) They are, however, the exception overall.

[7] Coercion is a staple of international politics and economics. The western powers after WWII certainly used the full range of fortunate circumstances, hard and soft power -- short of going back to war -- to achieve acceptably their goals for the international system. (Blanchard and Ripsman 2008) (Keohane and Nye 1977) Cyber coercion emphasizes deception in tools and opaqueness in originators across STESs and nations, making defense and public resistance difficult for the relatively transparent democratic nations. (Demchak 2013)

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

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 and 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 wifi 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)

11. 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. (Zittrain 2006)

12. The security of fault-intolerant languages such as LISP cost more in commercial production, while the fault-tolerant languages externalized such costs onto the using society. (Johnson 2005)

13. 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)

14. 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)

15. Buried in the thinking of even the more libertarian of scholars is 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)

16. 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)

17. For a longer discussion of these systemic advantages, see (Demchak 2012).

18. 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 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 et al. 2013) (Singer and Friedman 2014)

19. 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)

20. (Richmond 2011; Schrage 2011) (Goodin 2010) (Ponemon_Institute 2012; Goldman 2011)

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'. (Gorman 2012) (Rogers and Ruppersberger 2012) (Rogers and Ruppersberger 2012)(Rogers and Ruppersberger 2012) (Rogers and Ruppersberger 2012) Hacking is increasingly so sophisticated 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. Human organizations were formed for certainty – i.e., critical 'foreknowledge' -- in gathering enough food and defending it, in keeping threats collectively at bay when sleeping, etc. In advanced nations, one tends to use the term security and forget that it really means certainty about a preferred outcome. To us, it seems strange that freed slaves would stay in place because the only certain meal or shelter was where they were, or that Egyptians having overthrown a dictator would shortly elect one of his cronies because they promised stability – i.e., certainty about what might happen the next day, which the Arab spring and freedom had not done. (Shin 2015) It is useful to remember this instinctive human reach for certainty buried deeply in national policies and choices. (Barrett et al. 2012)

23. 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.

24. 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 et al. 2011)

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

26. 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)

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. 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 and 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.

29. 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).

30. The term 'multistakeholderism' is a term becoming widespread during the ICT driven globalization surge from the 1980s–mid 2000s began in the 1980s and surged dramatically in the 1990s through the 2000's. (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 prosperity depends on both of them absolutely. (Calandro et al. 2013) For the IT capital goods industry, however, the borders and the values issues are not interlinked. The business models only require no governmental restrictions on products and no hindrances in access to all markets, not for example universal freedom of speech. Many major IT corporates concede to Chinese requirements for compliance in technological surveillance of Chinese citizens or in sharing proprietary code in order to maintain their access to the large Chinese markets. (Tan and Tan 2012) (Jiang 2012) (Shih 2014)

31. Aided by the western corporate and individual state genuflection before that wealth. In this 2007 story, a major US toy corporation is said to be forced to apologize for harming the reputation of China's manufacturers when those factories used lead paint in the toys they produced. The consequences for not apologizing was, and always is, the indirectly given threat of losing access to China's market. (Story 2007)

32. One piece characterizes the Chinese internet as having "ossified into a highly regulated yet profitable info-web". (Schneider 2015)

33. Interesting enough, while some analysts argued the that China's People's Liberation Army (PLA) exploitation was declining over 2015, the Ministry of State Security (MSS) appears to have taken up the slack up to and through the signing as well. (Nakashima 2015) It is unclear what effect on Chinese cybered conflict hacking the massive 2015 OPM extraction of security data on over 23 million current and former US government employees will have. Digesting all that material could slow the development of operations as the unprecedented wealth of personal data offers Enigma-like intelligence opportunities, especially in extensive social engineering operations. The material will be used eventually. Employees can change passwords, but not their family history, dates of birth, etc.

34. 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)

35. 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.

36. A number of sources argue that the Chinese extraordinary economic advance from the rise of telecommunications giants such as Huawei and others has been fueled by stolen intellectual property, business intelligence, and rather well-established practices from bribery to blackmail. When whole proprietary products show up in massive production in China and then drive western producers out of business, Chinese rise merely through solid market performance is harder to prove. (McConnell et al. 2012) (Nakashima 2013) (USCESRC 2014; Hannas et al. 2013) (Hannas et al. 2013)

37. Russia's latest military doctrine explicitly includes as an integral part of modern warfare a total system battle, and the operational use of information weapons to create dissent in an adversary's nation. https://www.swp-berlin.org/fileadmin/contents/products/comments/2015C09_kle.pdf.

38. This hard turn in China's foreign behavior is palpable across a variety of areas from maritime demands to aggressive and dismissive behaviors in international conferences on internet governance. Long-term China observers have begun to publicly discuss their own wake-up moments in seeing a newly assertive China consciously and publicly rejecting the path to a democratic civil society. (Pillsbury 2015)

39. The role of India as a largescale nonwestern democracy in improving the odds for the long-term survival of democracies globally is woefully understudied. It is not included in this ten percent figure. (Stuenkel 2013)

40. 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)

41. Increasing the sense of surprise that could feed outrage and poorly considered policies is a US international relations literature largely is silent on adopting to the serious possibility of US decline, denies it, or bewails some aspect of it while calling for action to maintain the US's central role in the world. (Friedman 2010)