Military Cyber Affairs
The Journal of the Military Cyber Professionals Association
ISSN: 2378-0789

Volume 3 | Issue 1 Article 6

2018

Three Futures for a Post-Western Cybered World

Chris C. Demchak
U.S. Naval War College, chris.demchak@usnwc.edu

Three Futures for a Post-Western Cybered World[1] [2]

Chris Demchak[3]

Abstract: West faces a different security dilemma due to the shoddy cyberspace substrate it built and spread globally. Cyberspace created a new form of 'cybered conflict' with five advantages for offense previously – scale of organization, proximity, precision, deception and tools, and opaqueness in origins. It also accelerated massive wealth transfers to rising near peer and now peer adversaries, who were expected to simply fold into the western-built international system. In the process, the basic well-being of the economies of the consolidated civil society democracies have become non-kinetic fields of conflict among state and nonstate actors. The past twenty-five years of evolution of cyberspace have changes the currently likely futures of the democratic state and a rising post-western, authoritarian world.

Today in the emerging cybered conflict world, there are three plausible and distinctive futures for the international system, as well as for the relative influence and well-being of the minority of states that today are civil society democracies. Two of the three offer relatively grim prospects over time, leading to a creeping enfeeblement as individually weak cyber powers in a state of modern digital subordination to a much larger, globally omnipresent, authoritarian cyber and economic hegemon. There is a possible third option: an operationalized structure for sharing cyber security and defense. This third future needs to be actively built as was the shoddy internet that has made it necessary. And it needs to be built now before the full consolidated development of the global Cyber Westphalian system.

[1] *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.*

[2] Please cite as Demchak, Chris, "Three Futures for a Post-Western Cybered World," in Demchak, Chris C. and Benjamin Schecter, eds. *Military Cyber Affairs: Cyber, Economics, and National Security*3, no. 1 (2018).

[3] RDML Grace M. Hopper Professor of Cyber Security and Director, Center for Cyber Conflict Studies (C3S), U.S. Naval War College

Cyberspace is changing the international system, enabling the rise of a post-western, deeply cybered, and more authoritarian world order. Due to the shoddy coding of the basic internet global 'substrate', a wide range of malicious state and nonstate actors now have five unprecedented offense advantages in removing wealth and capacity from western democracies in particular. They can cheaply organize (at any *scale*) and use at any distance (*proximity*) any collection of cyber means (*precision*), with obfuscation in tools (*deception*) and in sources (*opaqueness*). The emerging era has ushered in a new form of system versus system 'cybered conflict' among states and their proxies or fellow travelers in which all five of these advantages are routinely involved.

For open internetted and democratic societies, the resulting volume of cybered economic losses alone have become a special strategic vulnerability. Recent estimates put these losses at an unsustainable 1-2 percent of annual GDP for US and its allies. (PWC, Hathaway) The easiest way to dismantle a democracy is to destroy its economic wellbeing and thereby the trust, transparency, and tolerance of its citizens toward each other and their overarching societal institutions. By undermining the long-term health of each nation's economy, this "cybered conflict" has become an existential challenge for democracy in these countries.[4]

Today the global system is no longer meta-stable with western powers willing and able to force other nations' compliance with westernized, civil society rules. Unlike the optimistic presumptions of the early post-Cold War era, the international system's evolution is no longer deterministically converging on common westernized rules of fair exchange. Reciprocally recognized and legally enforced contracts and relatively free trade across borders are eroding. Production successes and market fluctuations no longer reliably correlate with long established patterns in economic algorithms and analyses built on a century's worth of capital and labor ratio data driven by western economies. Globalization per se has stalled. The militaries of the modern civil societies are scrambling in preparations to defend their nations in electromagnetic and internetted space as well as in physical and territorial space. But the battlefield of the global system around them is altering. The odds of the current operational plans being successful are declining,

[4] '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)

DOI: https://doi.org/10.5038/2378-0789.3.1.1044

as more and more of the critical infrastructure of the defending societies is digitized and made vulnerable.

Representing less than ten percent of the world's population today, consolidated democratic states will in future have ever more limited capacity to drive what the rules governing what the remaining ninety percent of the globe's population does in with the cyberspace substrate underpinning global interactions.[5] The westernized states will no longer dominate global internet freedom, the international protection for rights of the single individual, the development, production, and uses of technology, or the rules of the international economic system. *The open question is not whether the democratic civil societies can rule the future international system, but to what extent the rising and largely authoritarian rest of the world rules the economic wellbeing, future political stability, and cybered defense options available to the outnumbered democracies.*

Three Futures

Today three distinct and plausible futures can be identified for the global system, each varying the relative strength of western civil societies to defend their economic wellbeing – and thereby their sovereign ability to determine their survival as democracies – in a conflictual cybered world. The three are entitled 'Cyber Status Quo' (CSQ, a continuation of the chaotically jostling states of today with continuing hollowing of democratic influence and coffers), 'Cyber Westphalia System' (CWS, each state defending alone and systemically vulnerable to creeping cyber subordination by an outsized largescale cyber hegemon), and 'Cyber Operational Resilience Alliance' (CORA, a collective whole-of-nations integrated response across integrated allied democratic civil societies). Each future suggests stridently different topological distributions of international power and economic wellbeing. Each has a different likelihood of democratic nations being robust cyber powers by midcentury.

The futures vary across two axes: sovereignty and scale. First, states array themselves a range in national efforts to legally recognize a home state's cyber sovereignty – i.e., its domestic cyber jurisdictional control – from none to national to shared. Second, states vary in terms of the scale of the cyber self-defensive resilience – the systemic resources mustered against external sources of cyber conflict and economic pressure – from none to solely national to shared. The axis

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

of cyber sovereignty at its lowest value represents a government making no effort to defend its national economy from an open internet's economic predation by external actors. The scale axis represents the state's ability to gather and effectively integrate sufficient demographic talent in information technologies and equally commensurate economic resources to defend itself against the globally huge mass of state and nonstate bad actors increasingly influenced by an overwhelmingly larger and rising 'cyber hegemon',[6] China.

As depicted by figure 1, these futures hinge on what western democracies do soon about their cyber sovereign jurisdictions and how they individually and collective respond to the scale challenge of the larger authoritarian world. There is little doubt, the future shared internet, global markets, and international institutions making the global rules of the road will be dominated by non-western autocratic states especially influenced by the largest of these nations – China.

Cyber **Sovereignty** Recognized **Scale** of Cybered Defense	LOW	HIGH
LOW	***Cyber Status Quo***	***Cyber Westphalian System***
HIGH	*Western Rules for International System (expired future)*	*Third Option??*

Figure 1: Two Futures and the Missing Third

Future 1: Cyber Status Quo (CSQ) – no sovereignty, no defensive scale

This future is already emerging if nothing changes from current operations among these states. Whether democratic or not, states that insist on maintaining the current and societally

[6] Chinese authors do not call themselves a 'cyber hegemon', and even argue the rising China will be the opposite. However, when Chinese President Xi declares the intent to be a major cyber power, the scale of the nation and its already demonstrated ability to pour vast funds into dominating IT sectors – while demanding adherence to its preferences – suggest the term will apply in any case. See (M. Liu, 2010) and (Blackwill & Harris, 2016)

unprotected, and open national cyberspace will experience the most abuse, exploitation, and loss of national wealth. They will be open to all malicious actors able to use the five advantages against the domestic assets of the outnumbered, consolidated[7], democratic civil societies. For these completely open and individually small states, the Cyber Status Quo future is likely to simply overwhelm their freedom of action.

Already the poorly built open internet has allowed a long-term campaign of economic attrition to be pursued against western states by adversaries, especially China.[8] Part of the explanation for the civil societies' laggardly responses to the cyber threats to the national system lies with the legacy economic models becoming dominant during the Cold War era. During that period, western powers dictated the rules of the international system without much opposition; the peer states that could have objected – USSR and China – had self-isolated economically to develop their versions of communist economies.

These westernized theories therefore came to dominate thinking about national macro and global trade economics in the artificial "Cold War" era. The societal and legal values of less than ten percent of the world's population came to be taken for granted as inevitable and immutable. It is arguable whether the basic western economic models' ever operated in reality as they were presumed to do during the Cold War and the immediate postCold period.[9] However, it is increasingly clear they are not fit for purpose in a rising age of cybered conflict involving the economic lifeblood of western economies surrounding by an emerging, much larger, and authoritarian world.[10] Industrial age theories of economics rest on key assumptions about the

[7] 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)

[8] To be fair, China is more of a "strategic opportunist" in that China has been able to exploit the blindness of western commercial and political leaders because the legacy economic theories and economists portrayed the extractions as minor issues in otherwise normal but vigorous interstate economic competition.

[9] For a discussion of this lack of applicability of current models, see the article by Harvey in this issue.

[10] Modern economic theory built in splendid mathematically pure theory and models isolated from real world conflict and politics serves its societies poorly if the nation's critical resources are being extracted in reality through mechanisms unexamined in theory and excluded from the idealized markets of the elegant analyses. (Keen, 2011) Furthermore, the models incorporating these assumptions are deliberately streamlined and reductionist for mathematical elegance, externalizing wider systemic conflicts out of the economic analysis and leaving their complexities to other fields.(Akerlof & Shiller, 2015) Exploits, abuse, and systemic harm travel easily across a globally open cyberspace substrate underlying the modern and modernizing nations. They spill over into the increasingly integrated domains of economic, political, and military actions and affect the major elements of a tightly coupled national system.

international and domestic systems. Among these are presumptions about stability in standardized and nonarbitrary rules of exchange, about ability of civil society to enforce transparency and legal recourse in contracts, about the availability of reliable data for value assessments and market impartiality, about non-arbitrariness in access to production and market processes, and finally, about rational – in westernized terms – human decision-making. In a rising authoritarian and deeply conflictual cybered world, these strongly westernized assumptions increasingly are unlikely to apply.

Today's cybered world is not forgiving of legacy thinking and laggardly responses in national defense. In this and the second of three futures, the westernized civil societies will suffer the worst for such shortcomings – for refusing to see a need for a state to defend its cybered economy at the scale required. As previously noted, western states already experience levels of annual GDP losses due to cyber insecurity, that are unsustainable over time. (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) It is not clear where the tipping point lies, but it is likely there is one after which a state committed to this kind of future may no longer be able to change its course and still have the capacity to defend its wellbeing.

Future 2: Cyber Westphalia System (CWS) – sovereign jurisdiction, no defensive scale

States that do recognize the need for defensible cyber sovereignty but who attempt to individually defend their own jurisdiction will not, in principle, be as exploitable as the completely open states. However, they will be at the mercy of the scale of authoritarian demographics, whether democracies or not. For democracies in this Cyber Westphalian System, however, this new dominant global meme will be led not by the civil society rule of law of the Cold War, but largely by diversity of authoritarian leadership styles, ranging from the Putins to the Assads to the Xi Jinpings of the world.

The difficulty is that the rise of the 'rest of the world' (ROW) was inevitable, but the loss of global control by westernized democracies happened much faster and more pervasively than might otherwise have occurred if there had been no – or a different form of – cyberspace. The speed has left the civil societies stunned. The push towards a defensible national cyber jurisdiction has accordingly been slow as political and commercial leaders still embrace the legacy and

widespread 1990s utopian views of the internet. These misperceptions were themselves the result of an enduring, industrial age libertarian, and corporate commercial fixation that prioritized market access over national or systemic security, underlain by an overarching political complacency across western states about the inevitable domination of their vision of democratic civil society and international rule of law.

In reality, each lone nation trying to defend its own cyber jurisdiction today faces an overwhelming tide of autocratic, anti-democratic, and industrially arbitrary forms of societal control now more effectively pervasive and digitized. Cyberspace has accelerated intra – and inter – state economic exploitation and reinforced the wealth extraction and societal control of personalized political control across the non-westernized majority of the globe. Chinese scale in population and in digitization, and in ever-growing cybered conflict skill challenges democratic societies' influence over the interstate system. China's defense of its national cyber sovereignty is likely to be the dominant model for all nations. Although the major cyber 'authoritarian anchor' state, however, China has a strong interest in ensuring its own economic wellbeing, irrespective the effects on the wider system. It already has its own legions of cyber black and grey actors able to exert economic pressure on a global scale, along with digitally extracting and extorting resources when and where desired.(Wang, 2017)

Furthermore, since the bulk of the world tends toward authoritarian political cultures and structures, China will as an extremely largescale, coherent, determined, single actor be particularly able to channel – if not dictate – the rules of economic exchange and wealth concentration in practice across the international system by its presence ubiquitously and its deeply embedded regional, economic, and cybered bonds. Of course, in this Cyber Westphalian world, authoritarian states will also lose their economic wealth and relative power to resist external pressure. They will not be the major targets, however, until after the wealthier democratic states individually have had to concede to the cybered conflict campaigns of China and its allies – especially its expression in aggressive economic statecraft. (Reuters, 2017) (Blackwill & Harris, 2016) (Mastanduno, 2005) (J. M. F. Blanchard, Mansfield, & Ripsman, 1999)

At present, the two futures most likely – a continuing Cyber Status Quo, or an emerging Cyber Westphalian System – suggest the coming era is on its way to being more like Sino-centric economic-political control than the post-Cold War US dominated new world order. (Ringmar,

2012) As a result, two of the plausible three futures are grim indeed for the long-term survival of civil society states as democracies. Each suggests for the minority of states that are consolidated democracies a form of cyber economic subordination – a creeping loss of independent economic wealth and defense capacity in the coming cybered world system. CWS appears more likely because cyber borders are rising globally, even piecemeal among democracies. 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 national servers, and yet others in the form of indirect access and content controls executed through controlled browsers, subscriptions, or identification tagging and logging. (Deibert & Crete-Nishihata, 2012) (Dombrowski & Demchak, 2014) With other authoritarian states, China never gave up its domestic control on internal communications systems and 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.

At the end of the day and so far, 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 cyber borders does not 'break' the internet and destroy its generativity as western policymakers and technology private sector leaders warned. Instead, overt and latent authoritarian national leaders have been emboldened because of the apparent Chinese success while controlling their domestic cyberspace, and the Cyber Westphalian System is emerging rapidly.

Search for an Alternative to Futures 1-2: Geopolitical Considerations

Cutting across all these futures is the question of how western defenders are to construct a third and more acceptable future – one that resolves the overwhelming threat to an open and unexploited, productive internet posed by the scale of a rising authoritarian world not bound by the westernized civil society rules. This challenge is larger than that posed by the relatively less complex bipolar Cold War. Economics and democracy are intimately bound; the easiest way to destroy a democracy is to destroy its economic system and the tolerance among groups within the

DOI: https://doi.org/10.5038/2378-0789.3.1.1044

society. Cyberspace furthermore has enmeshed the economic effects with the effectiveness of the military's contribution to the defense of the nation in ways unimagined in the early euphoric infancy of the internet. Irrespective of preferences of the westernized states' political, military, and private sector leaders, China will continue to rise as the emergent cyber hegemon. It will turn to use its physical proximity, historical ties (including subordination) and its baseline technological controls of the networks and portals underpinning national economies to create hegemonic spheres. To a lesser extent, Russia will attempt this as well, further fragmenting the wider more authoritarian world into a larger mass response more to China and possibly a smaller group tied culturally to Russia and other minor cyber economic powers.

As a class of nations, the authoritarian states will all use the reach of the cyberspace substrate to politically and economically coerce preferred behaviors from subordinated nations or groups. For example, China would use the socio-technical-economic leverage provided by the previous twenty odd years of Huawei building for free the 4G networks of nations from Laos to Bangladesh to Kenya to Angola, and multiple nations in-between. With these embedded economic reigns, China will have the influence to pre-empt – or punish – any behaviors deemed inimical to its notions of a China-friendly cyber buffer zone or viewed as a lack of respect for Chinese major power interests. Russia will attempt to do the same for its near abroad, although it is not clear how successful Russia will be as a 'Net Hegemon'. It has no state corporate champion like China's Huawei that is building for free and operating national networks across the nations it would like to have as cybered subordinates. Russia could more easily become an irascible independent cybered state as first among equals among nations on the peripheries of western- or Sino -oriented states. For Russia, its natural – if possibly ephemeral – community may be the prey to larger, more coherent cyber states, especially China: i.e., all the ungoverned, war-torn, demographically debilitated or ruinously underdeveloped nations who will have the pro forma recognition of a national cyberspace without any hope of actually controlling it completely.

If no third alternative future may be found to resolve the scale shortcoming of the western-oriented societies, the future cybered international system is likely to operate along the lines of the Chinese cultural preferences and the examples given by its recent history. In Chinese society, its organizations, and its business practices, hierarchy is preferred uniformly. Size makes right – the big are entitled to compel the small. History trumps law unless the law's verdict suits the

preferences of the one at the top of the hierarchy, i.e., China.[11] (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) (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,

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

DOI: https://doi.org/10.5038/2378-0789.3.1.1044

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, in 2017 major South Korean firms suddenly experienced 'difficulties' in their Chinese operations when South Korea and China relations hit a downturn. (Jin, 2017)

In this coming international system, a minority of westernized democracies will be challenged to avoid being economically and then politically coerced over time. Scale needs to be met by scale, or the challenger needs to change the conditions of key aspects of the competition. The alternative is to eventually concede to a global version of China's "info-web" internet as a cyber economic subordinate unable to effectively refuse direct or indirect coercion from the cyber hegemon. (Schneider, 2015) The first two of the futures are the most likely if nothing about the systemic scale of the defense changes from current operations among these states.

Future Three: Cyber Operational Resilience Alliance (CORA)

Changing the conditions for the future means creating the necessary scale by accumulating cyber sovereign defensive capacity across like-minded democracies in an institutionally and technologically integrated 'cyber operational resilience alliance' (CORA). This plausible future is the only one that could conceivably 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 – even if only for these nations within the alliance. It is the only future that offers the breathing space by which the originators of the shoddy internet develop the IT innovations to remake the underlying substrate properly. Only the dedicated efforts across these nations can succeed in saving their internet by transforming it technologically, societally, and economically as it was intended, and defending it while rebuilding it even if only for themselves. Since trust will be critical, cultural correlates and historical ties (path dependence) will really matter in this conflictual and deeply cybered world. Most of the allies are already able to trust each other in shared forums such as NATO and the EU; they already have the experience of successful defensive

communities. As shown by figure 2, an alliance has the best possibility of creating the missing scale needed to successfully resist otherwise overwhelming authoritarian pressure.

Cyber **Sovereignty** Recognized **Scale** of Cybered Defense	LOW	HIGH
LOW	***Cyber Status Quo***	***Cyber Westphalian System***
HIGH	*Western Rules for International System (expired future)*	***Cyber Operational Resilience Alliance (CORA)***

Figure 2: Three Futures

Achieving this future will be challenging. At least four primary actions must be taken. First, a major part of the necessary response is to alter the cognitive framing created in the early frontier era of cyberspace deifying a completely open global and government free commercialized internet and imbuing it with magical utopian properties. (Rheingold, 1993) The reality of a rising Cyber Westphalia System of national jurisdictions must be recognized and accepted. 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 no chance of emerging along with a rising authoritarian rest of the world. Chances to slow this rise of cybered conflict have been squandered.

A range of missed technological transformation, societal resilience, markets reform, and informed policy opportunities have been lost. That doggedly western civil society narrative now has a major counter-narrative – one that is well funded, covertly reinforced, and overtly widely promoted from a rising and confident large authoritarian actor, China. It is a new narrative that is attractive to a larger authoritarian world and changing the realities governing the future cybered world. Cyber jurisdictions are emerging whether or not the westernized world desires them. Continuing to oppose the process by democratic leaders simply accelerates the likely affiliation of the rest of the world with the Chinese model.

Without this recognition of a national cyber jurisdiction, democratic leaders cannot use "stateness"[12] – a sense of collective willingness to act – to create and sustain systemic resilience across society including its private sector. 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.[13] 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 and spread that model globally.[14] The idealized westernized open internet model already lacks strong examples of success without being economically plundered.

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.

An 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 forms of authoritarianism emergent today. After the Cold War, however, these states still expected their global dominance to continue and never recognized it as both very shallowly adopted by many nations and deeply 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

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

[13] 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).

[14] 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)

blend of historical trends involving Roman Army impersonalized organizations, Catholic transnationalism and social marketing, Protestant societal leveling and internalized ethics, and the Enlightenment. (Goldstein, 2015; Tilly & Ardant, 1975)

Third, the alliance requires acceptance of the power of demographic scale; it is the key distinction recognized by China as meriting any nation peer status with Middle Kingdom. 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 struggling as singletons to defend their own national cyber jurisdictions, each alone has 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 socio-technical-economic systems (STESs) will be unsustainable if every state is to independently afford and orchestrate advanced technologies, resilience budgets, and collectively intelligent choices.[15]

Fourth, the alliance must be large enough to be recognized as feasible. The community of consolidated democratic states estimated at 30-40 states has collectively about 800-900 million people in well-educated modern communities.[16] This demographic scale is sufficient to be relatively economic autarkic in IT investments and production if need be. It is 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. These minority states have the resources to create a coherent entity able to defend these cybered STESs jointly.

The alliance reaches well into the private sector as well as governments. There is nothing magical about the authoritarian states turning to their existing telecommunications agencies – often recently renamed corporations – to deepen governmental cyber controls. Consolidated democratic civil societies also have centrally situated backbone telecommunications firms that used to be singleton national agencies and still need to be enlisted in the efforts to build the cyber resilience

[15] 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)

[16] Ultimately India's demographic weight will be critical to the survival of the democratic model globally. However, India is developing as a fully consolidated democratic civil society. At the moment, the advanced democracies must secure their own collective cyber resilience scaled to their own economic and political wellbeing before being strong enough to help India secure its cybered future. Hence, its demographic weight is not yet included in this assessment. It is not if India as a democracy joins this alliance; it is a matter of when.

DOI: https://doi.org/10.5038/2378-0789.3.1.1044

of their community. But democracies also now have the larger IT capital goods private sectors. These are likely to lose both their access to large authoritarian markets in the future. As the Chinese model demonstrates, western global competitiveness dramatically wanes when nondemocratic nations close their cyber national borders close and impose internal national policies extracting 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. As they recognize their long-term interests – and the alliance's internal market size now reserved for them, they are more likely to be receptive to realizing they too are integral to this alliance. In any case, the larger world's cyber hegemon itself has no intention of allowing the currently dominant westernized corporations to maintain their global markets in a Sino-determined future.[17]

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 having 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 two player competition present between NATO vs Warsaw Pact to buy time. The alliance is needed in the near term to buffer the democratic societies while their collective talent innovates 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, operational alliance of mutual systemic

[17] See for example the Chinese plan to be the dominant technology economy by 2025. (Yuan, 2018)

cyber resilience. In recognizing the existential long-term trends and competently defending the interlinked STESs, these nations can change the current trends, and create a third more positive future. In this way, they can increase the odds of surviving collectively as robust cyber powers adequately prosperous in trade and wellbeing, and still be consolidated democracies over the long term. Alone, none of these nations will do well over time. And, there is not much time left.

DOI: https://doi.org/10.5038/2378-0789.3.1.1044

REFERENCES

Akerlof, G. A., & Shiller, R. J. (2015). *Phishing for phools: The economics of manipulation and deception*: Princeton University Press.

Blackwill, R. D., & Harris, J. M. (2016). *War by Other Means*: Harvard University Press.

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

Blanchard, J. M. F., Mansfield, E. D., & Ripsman, N. M. (1999). The political economy of national security: Economic statecraft, interdependence, and international conflict. *Security Studies, 9*(1-2), 1-14.

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

Chang, A. (2014). *Warring State: China's Cybersecurity Strategy* Retrieved from http://www.cnas.org/chinas-cybersecurity-strategy#.VeHZlM5REr s:

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

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

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

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.

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

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

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

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*.

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.

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

Keen, S. (2011). Debunking macroeconomics. *Economic Analysis and Policy, 41*(3), 147-167.

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.

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

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.

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, M. (2010). *The China Dream*: Beijing: China Youyi Press.

Mastanduno, M. (2005). Economics and Security in Statecraft and Scholarship. *International Organization, 52*(04), 825-854.

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

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

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

Reuters, S. (2017, August 21). Don't like our rules? Then leave, China newspaper says Western institutions don't like the way things are done in China they can leave. *Reuters online*.

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

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

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

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

DOI: https://doi.org/10.5038/2378-0789.3.1.1044

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

Wang, Z. (2017). The Economic Rise of China: Rule-Taker, Rule-Maker, or Rule-Breaker? *Asian Survey, 57*(4), 595-617.

Yuan, L. (2018). Why Made in China 2025 Will Succeed, Despite Trump. *New York Times*.