Integrating thinking

Cybered conflict, cyber war, the Russian ‘hybrid war’ (Chivvis, 2001), and even the Chinese ‘wars under conditions of informatization’ (Polpeter, Chase & Heginbotham, 2017; Kania & Costello, 2018), all reflect the emerging reality of conflict among states in a deeply cybered, non-westernized world. Throughout history, the keys to conflict, competition, or war are the scale of available, relevant foreknowledge and of applicable resources to act accordingly. They are the critical ‘knowing and acting’ of all struggles, but in the emerging era, the volume of both foreknowledge and resources required is unprecedented. If one is constantly open to nasty surprises that can be imposed ubiquitously from one’s critical complex systems and one cannot gather the resources needed in time to mitigate, neutralize, recover from, and innovate beyond, the surprises imposed by adversaries, then one faces both exceptional uncertainty and wartime-levels of insecurity. Irrespective of what that struggle is called, one is then likely to lose in conflicts involving cyberspace. Just as in other eras and contexts, security in cyberspace is therefore not the absence of threats, but the inability to minimize either or both systemic uncertainty and the magnitude of significant harm associated with threats.

The current form of the global cyber substrate encourages long-running and obscured digitally-enabled contests that systemically blend uncertainty and insecurity. It offers five offense advantages for aggressive actors to employ in imposing their preferences on defending actors’ nation-wide socio-technical-economic systems (STES) (Demchak, 2012a). The multiplicative ways these five offense advantages – scale in organization, proximity, precision, deception in tools, and opaqueness in origins – can be employed in cyber campaigns has led to considerable confusion in terminology, observation, and weak theorization. Over the past decade, an explosion in debate the elements of the global internet and related technologies has produced an equally confusing number of new terms or labels. Practitioners and scholars alike have engaged in a good deal of ‘facet learning’, i.e. studying and reporting about one or two facets of a larger and much more complex whole without taking the final step of combining the facets. Missing is consensus about the basic
nature of conflict through cyberspace. We lack an approach that helps explain conflict that is ‘cybered’ and its evolution.

This chapter aims to clarify the field by offering one basic term for the conflict now exploding in, through, and enabled by, cyberspace – ‘cybered conflict’. It is a form of large-scale intergroup or interstate struggle whose outcomes critically depend on the involvement of cybered means and whose activities lie upon a spectrum of traditional peace to war reaching all levels and actors in a state’s socio-technical-economic systems (STES). The goal here is to advance thinking systematically on the concept in order to promote better integration of a widely diverse array of arguments from differing disciplines, including economics which has eschewed directly addressing cybered conflict. This contribution is midlevel theory, offering the basic elements by which to move beyond mere observation to theoretically and practically framing productive, feasible implementations – to develop an integrative approach to both ‘knowing and acting’ in cyberspace for nations defending themselves in these struggles.

Four arguments will be made. First, cybered conflict’s central pursuit is the aggressive acquisition of access to accurate current data to ensure the overwhelming foreknowledge needed to control outcomes of a nation’s complex STESs. It is closely married to a virtuous loop in which more data means more resources, and more resources funds the acquisition of more data – as well as the available assets for action on the foreknowledge developed. That is, the cognitive – or ‘knowing’ – aspects of cyberspace ultimately will determine the uses – or ‘doing’ – to which its connectivity and content are put (Kuehl, 2007).

Second, the shoddy creation of the current cyberspace made this central pursuit much easier by expanding to a massive community of bad actors five offense advantages traditionally held largely by emperors and close neighbours. Put in other terms, emperors by the vastness of their resources could mass large armies, move great distances, apply a wide variety of weaponry over time, imperviously replace any lost resources, and remain at their home base immune to punishment or retaliation. Now any group of bad actors with access to the internet and time can execute cybered conflict campaigns using those advantages for minimal expense and with impunity.

Third, those states able to continually amass extensive foreknowledge of their own and of other states’ STESs – as well as the resources at scale to aggressively act in offense and defence – have underlying advantages in cybered conflicts. These are more likely to develop as cyber powers. The more robust the cyber powers are – i.e., the more state leaders manifest strategic coherence and appropriate scale in successfully developing national systemic resilience and legal forward disruption capabilities as needed, the more likely those states will prevail either as aggressors or defenders.

Fourth, the current world of cybered conflict is sorting into two futures. The most probably is a China-centric global system with minimally remaining, concrete democratic civil society influence. One aggressive, authoritarian actor – China – has already demonstrated the scale in resources (especially demographics) and strategic coherence in leadership to determinedly pursue systemic foreknowledge and to act institutionally on the data acquired globally. The fragmented and often fractious minority community of consolidated democratic states do not have individually either the scale of resources or strategic coherence necessary to prevail over time in cybered conflict given current trends that. Another possible future assumes that the rise of China cannot be contained in any case, but that there is a conceivable wary for the minority community of democratic states to persist in offering the world an alternative model. This future is only reasonably possible if these states make an existential choice to collectively erect a strategically coherent, cybered ‘peer’ institution to
defend and nurture a competing, completely transformed and economically vigorous cyber-space along democratic values and preferences.

This new world’s struggles will move faster, hit further, change elements more profoundly, and amplify more broadly with more existential consequences precisely because of the new importance cyberspace awards to large scale acquisition of foreknowledge and resources married to STES strategic coherence. To date, democratic civil societies as a whole have been confused at best, complacent at worst, in dealing with this new world, their new role as a minority community, and the deep challenges to the assumed permanence of their global dominance and of democracy itself. This chapter offers an integrated way to view what has changed, what is happening, and the stark choices ahead for these societies and their thinkers in the coming deeply cybered world.

Aggressive acquisition of foreknowledge

Adversaries – whether state, proxy, or merely business competitors – have always sought information in advance to augment their own chances of prevailing in any form of contestation from war to gang or mafia deals to legitimate and rule-based markets (Handel, 1989). Having accurate data on what adversaries are planning to do, when, where, with what or whom, for how long and to what end is the gold standard of intelligence collection giving better chances of prevailing in pending, possible, or plausible struggles with others (Keegan, 2004). The more complex and surprising the world surrounding competitors is, the more critical it is for adversaries to acquire and analyse vast amounts of data to provide accurate foreknowledge (Betts, 1982). In the cybered world, electronics are critical to the collection of this foreknowledge and, hence, to the cognitive analyses behind decisions in any form of competition or conflict (Arquilla, 2009). The further today’s cyberspace spreads into all levels of any society, the more access points and systems a society’s adversaries could penetrate and ‘p0wn’ (Oren, 2010) in the defending society’s underlying cybered systems. It can be quite difficult to secure knowledge, especially it is transmitted to others; even verbal conversations can in principle be tracked by cameras and long-range listening devices (Riley et al., 2005). Even posted paper mail can be tracked digitally through a set of postal centre servers capable of reproducing a trail of probable communications between endpoints (Gill, 2006). Everywhere that information can be obtained remotely through digitally enabled means has become a possible target for adversaries’ campaigns for foreknowledge.

Among state level adversaries especially, every aspect of the opposition’s national social, technical, and economic sectors is in play, making cybered conflict a particularly broad-based system-versus-system struggle (Gilpin, 1981; Nye, 2017). Even the communications essential to commercial relationships and western markets – long considered during the Cold War and its aftermath to be off the table in national security discussions – have become part of campaigns to obtain foreknowledge for possible control of defenders’ resources (Wilber, 2018).

One major state actor, China has a well-established reputation for aggressive and blatant foreknowledge acquisition campaigns (McConnell, Chertoff & Lynn, 2012). Its industrial industries’ blatant tendencies to copy and market technologies by reverse engineering was so well known even in the 1990s that the agreement to let China join the World Trade Organization (WTO) in 2000 rested on Chinese promises to fairly open its markets to all investors and close off state subsidies. The Chinese market’s enormous scale loomed so large that the fact that China nonetheless pursued technology and market foreknowledge aggressively was ignored by potential western investors for years. While continuing to violate its
WTO promises, China has advanced economically in considerable measure by requiring foreign firms to hand over their technical data – now including source code – in trade for access to Chinese consumers. It has refused to prosecute violations of international economic standards, including remote or insider theft of critical data from westernized industrial, technological, and other economic systems (Atkinson & Ezell, 2015).

Furthermore, this aggressive acquisition of data is embedded in the international business models of China’s commercial ‘state champions’. Those leaders fully understand the personalized and broader five-year strategic expectations that they will rise to dominance in their sectors in order to justify the national support they received (Li, 2016). To that end, vast amounts of resources are spent and enormous efforts to acquire foreknowledge have been aggressively pursued, particularly for the past fifteen years (Zhou, Lazonick & Sun, 2016). Repeatedly, Huawei – the Chinese telecommunications equipment state champion along with ZTE – has been accused of stealing massive amounts of intellectual property in the markets in which it has steadily risen, especially telecommunications backbone equipment (DOJ, 2019).

Westernized states, especially the United States, have also vigorously pursued foreknowledge of adversaries through digitized data acquisition, but not systemically on everything, especially corporations and citizens. Due to civil society restrictions, intelligence operations are generally narrower in scope. Forward searches tend to focus on foreign governments specifically (Nakashima, 2008). The central locus of computer knowledge in the US – the National Security Agency (NSA) – is restricted from any domestic collection of data. In the early 2000s and in order to catch terrorists inside the homeland, the US government proposed a more systemic domestic government data collection plan – Total Information Awareness (TIA). It was met with both ridicule, vigorous legal objections, and cancellation (Poindexter, Popp & Sharkey, 2003). Commercial westernized entities such as Google, Facebook, and Apple have more access to wide ranging STES information – albeit on their own customers – than the US government does. However, they openly appear to fight government requests to share large portions of it, generally citing privacy and reputation concerns. More recently the European Union has elevated individual privacy rights through its GDPR regulation – including the right to be forgotten online. The result is to make vast amounts of systemic STES data unobtainable by EU national governments in general (Albrecht, 2016).

More recently developers of artificial intelligence – which requires enormous amounts of raw data on which its algorithms learn patterns and evolve decisions subsequently – have complained about the lack of available, real training data from all walks of life in westernized countries (Campbell, 2019).

As an adversary, therefore, China is likely to develop better foreknowledge of any given defending opponent. Not only is the Chinese vigorous program of AI development able to access massive amounts of data retrieved from abroad for training (Aitoro, 2019). China’s leaderships have also inaugurated a social credit system tracking the acceptable behaviours of every Chinese citizen from social media to economic exchanges (Qin & Hernandez, 2018; Wright, 2018). New regulations now require all Chinese firms to be willing to respond to Chinese government intelligence requests as needed (Bandurski, 2017). Chinese AI advances will have cumulative big data advantages in the near future that westernized democratic developers will have to create by simulation in hopes of matching the AI training sets and learning. Correspondingly, China’s political leaders have a greater likelihood of having a wider command of trends and decision concerns across leaders and STESs of other nations as its increasing mountain of data is processed more rapidly by its better trained AI algorithms.
Offense advantages from shoddy substrate

Globally critical to all the major sectors of nearly all societies, the underlying cyberspace substrate was built shoddily, written in quick-written, fault-tolerant code cheaper to produce and relatively easy to hack (Mills, 2010). The 1990s euphoric and naïve early days of the internet widely spread the idea that a brave new world of free, accurate information would ensue, making governments irrelevant, massively increasing prosperity for everyone, and assuring democracy as the dominant governance model everywhere the internet went (Rheingold, 1993; Norris & Jones, 1998; Benedict, 1991; Oyedemi, 2014).

The nascent commercial IT capital goods industry that built this insecure societal substrate did not see spreading democracy or security overall as their responsibility. Nor did the early internet seem particularly unsafe at the outset. Rather, information technology (IT) was promoted as historically special and unstoppable. The IT entrepreneurs argued their industry alone was – and should always be – free of government regulations because any restrictions at all would be harmful to innovation and the progress of the future world’s prosperity in general (Geer et al., 2003). The result was an explosive commercialization of the internet that was security-blind save minorly as a product functionality or a business intelligence issue. The web’s producers focused on commercial gains over competitors in speed of coding rather than quality. This argument – which continues today in the westernized states – adamantly opposed any government regulations requiring common standards for embedded security be met (Oxley & Yeung, 2001; Kinnersley, 2015).

The resulting substrate – poorly secured and oversold as it was – changed conflict by globally spreading five offense advantages that had previously been available only to wealthy emperors, superpowers, or close neighbours. With few resources save time and access to the internet, an aggressor can wield the superpower’s scale of organization through a botnet, live at any proximity from five hundred to five thousand kilometres from the victims and easily acquire previously high quality intelligence, and launch a variety of attacks at any level of precision in targets, time, duration, effects, or return benefits desired (Demchak & Dombrowski, 2011). Two more offense advantages developed as well: deception in tools and opaqueness in origins. Given the complexity of the global cyber substrate across cultures, governance, technologically diverse systems, and connecting protocols – plus the sheer volume of content per second, attackers have the opportunity to hide their tools to prevent interruptions or protections, and to obscure themselves to prevent punishment or retaliation.

These last two advantages are special bonusses for the average aggressor organization or even large states. Small or larger groups of bad actors may roam across the poorly secured global web and conduct attacks with impunity and a large potential for success. While historically a conventional attacker could not hide its weapons or generally its armies, in cyberspace both can be cloaked for a very long time.

With these advantages, attackers can be covertly hollowing or ‘poisoning’ the value chains sustaining the economics of a state for so long that whole nations could be losing a cybered conflict and not realize it. For example, automatic updates – a staple of today’s cybersecurity good practices – can themselves be corrupted, removing what is a basic line of defence against harmful losses from the web. For six months in 2018,

[s]omeone was able to modify a copy of the Asus Live Update Utility, hosted on the Taiwanese manufacturer’s backend systems, and sign it using the company’s security certificate, even keeping the file length the same as the legit version, to make everything seem above board. The update utility ships with every machine, and routinely upgrades...
the motherboard firmware and related software with any available updates from Asus. When it checked in with Asus’s servers for the latest updates, the utility would [automatically] fetch and install a backdoored version of the Asus Live Update Utility … between June and November 2018, according to Kaspersky. That infected build of the utility was designed to spy on roughly 600 machines, identified by their network MAC addresses hardcoded into the software. … [D]ubbed ShadowHammer … a very sophisticated supply chain attack … stayed undetected … [in large part because] … trojanized updaters were signed with legitimate certificates.

(Thomson, 2019)

The apparent ease of cybered conflict and the associated removal of data and thereby its economic value has elevated cyber insecurity to a tier 1 national security issue for major advanced economies (Cornish, Hughes & Livingstone, 2011). The losses from the economic sectors of the democratic civil societies alone are said to constitute the ‘greatest transfer of wealth in human history’ (Paganini, 2013). The French Senate has characterized these losses as the ‘pillage’ of the future of France economically (Bockel, 2012). In recent years others have estimated the losses to average 1–2% of the annual GDP of the advanced democracies (PWC, 2014). The estimates of losses have year on year been rising indicating a cumulative decline in the robustness of economic growth across the most targeted economies – the westernized civil societies (Verizon, 2017).

With these advantages intact as long as the current and shoddy structure continues, cyberspace changes conflict profoundly from the Cold War and its twenty-year aftermath. Cybered conflict now strongly influences the trends in the distribution of national economic, deterrent, and reputational power throughout the global system. From the 2010 Stuxnet (Gross, 2011), 2015 Black Energy (Liang et al., 2017) or the 2016 OPM data hack (Gootman, 2016), attacks sponsored by – and widely attributed to – other states are common without a victim nation’s leaders demanding national mobilization to militarily strike back at hosting countries. Today there is a rise in the destructiveness of attacks with losses that – though large in implications – still remain below the threshold of the traditional war defined by the Law on Armed Conflict (LOAC) (Schmitt, 2013).

More and more attacks simply destroy data en masse. In both the 2014 Sony (Sharp, 2017) (attributed to North Korea) and the 2012 Saudi ARAMCO (Bronck & Tikk-Ringas, 2013) (attributed to Iran) attacks, data was deleted, and computers destroyed. Ransomware (Everett, 2016), for example, was initially viewed as a nuisance when it surged several years ago. More recently, through badly or intentionally poorly coded ransomware, the effective destruction of data is rising because it cannot be decrypted. This development reached global proportions in major attacks such as the WannaCryPetya and notPetya (attributed to Russia) attacks mid-2017 (Simmonds, 2017). The 2017 WannaCry global ransomware attack, for example, effectively destroyed everything it encrypted, since it had no decryption for payment mechanism (Ehrenfeld, 2017; Romine, 2017) With limited personal costs to these attacks – especially if sponsored by another state – new and existing actors are emboldened in general to seek more ways to exploit the substrate (Sanatinia & Noubir, 2015).

The destructiveness of cyberattacks continues accelerating as aggressors test the limits of national tolerances for unconventional attacks and losses without directly responding through highly public and direct punishment. These attacks blend cybercrime tools with the whole-of-society cybered conflict and appear designed to coerce particular states or large economic actors into complying with the desires of the originating state without the proof needed to escalate into a kinetic war (Maness & Valeriano, 2015; Demchak, 2013).
Harder cyber hits – perhaps across more sectors or deeper in domestic infrastructure – are more likely if previous efforts are not perceived to have the desired effects of sufficiently harming their targets. Assaulted firms do not fold or seem to be punished existentially by stockholders – Sony still exists, as do the major WannaCry victims Maersk and Saudi ARAMCO. Large victimized firms continue today as if the cybered attack was of no consequence. In every other field of enquiry, such conditions—no repercussions for attacks and lack of evident harm in prior attack modalities—tend to increase adversary efforts to make the attacks more evidently painful. If merely losing money or risking client trust is insufficient, then the next – and already present – level involves destruction of something that systematically matters more than a single firm’s IP or financial resources. In addition to the now normal information disruption campaigns, Russia has been using cyberattacks on energy plants routinely for the past several years in the Russo-Ukrainian war with carefully timed and programmed outages. It now invades cell phone connections to identify grouped Ukrainian soldiers in the field for battlefield missile strikes (Haines, 2015; Limnéll, 2015). Cybered conflict is therefore moving more readily towards the destructive end of the peace-war spectrum as aggressor nations become more skilled in it – more robust in their cyber power, especially in using the five offense advantages.

Robust cyber power

Being a ‘robust’ cyber power strongly advantages an actor in this endless struggle for foreknowledge and resources among adversaries, enabling one a better chance to prevail in cybered conflict campaigns under current conditions. Power – whether robust or weak – is widely misunderstood. Unlike the Cold War and aftermath definitions, national cyber power does not solely depend whether a state has a vigorous offensive cyber program with a reputation for successful individual operations. Merely having a cyber command does not make a state a robust cyber power. Rather, in a system-versus-system conflict that moves along a spectrum of peace to war, cyber ‘power’ varies as well along the spectrum of competence in defending the national STES, in addition to any ability to operate beyond borders into other nations.

This competence is composed of two major categories of efforts – the systemic resilience capability of the entire nation (Hathaway, 2013) and the forward disruption capabilities of the government. Both are critical and must be balanced in order for a state to accumulate cyber power. In any case, the larger, more complex, more sieved, more diverse, and more digitally integrated the nation involved, the greater the strategic coherence – and the sheer scale in available foreknowledge and resources – are required to be a robust cyber power.

Either authoritarian or democratic states can, in principle, achieve this robustness, but most states of the world are, at best, weak cyber powers, even those with some solid reputation for offensive cyber capabilities (Martins, 2018). Robustness in cyber is determined systemically by state leaders and actions that exhibit strategic coherence in recognizing – and acting successfully upon – the need to orchestrate, nurture, and innovate the cyber security of their nation’s entire STES. This challenge was hard in previous eras, and has proven to date nearly overwhelming, especially for the open internet societies. For example, the continuing loss in GDP growth already noted is an indicator of the weak level of cyber robustness of these victimized and largely democratic states.

Defending one’s STES is particularly challenging for any state, especially those already under assault. Due to the inherent shoddiness of cyberspace, the general sources of harmful systemic surprise for modern democracies doubled in the past twenty-five years – from two
to four. In the pre-cyber era, complex societal surprises came from individual enterprises (layer 1) or from collections of independent enterprises (layer 2) commonly seen in critical infrastructure industries. With the cybered era, however, now reaching into the nation’s vital functions are a massive volume of independent, criminal ‘bad actors’ (layer 3) spread across the world, along with a much smaller more focused and organized group of exquisitely skilled ‘wicked actors’ or ‘wizards’ (layer 4) usually employed by states or international criminal organizations (Demchak, 2012b).

In particular, due to the five offense advantages of the current cyber substrate, it has proven extraordinarily difficult to curtail the inroads and successes of the bad actors and their wicked actor compatriots. The scale and coherence of effort needed has proven exceptionally difficult to rationalize at the strategic political level within national systems, and across the international community of nations (DeNardis & Raymond, 2013). The lingering early internet optimism has continued to stymie systemic and collective responses from democratic governments in particular. The westernized IT capital goods industry’s argument that government interventions will destroy IT innovation and stall the economy has crippled nationwide defence responses. Ignored is obvious contrary evidence from China readily available from open media reports for nearly a decade. China continues year on year to rise economically despite it having a controlled internet and requiring government equity in all IT industry firms. So strong are these early images of the great new internet-led world order that private sector actors continue to refuse to coalesce with civil society government over the strategic need for both to take responsibilities in protecting their collectively existential national cyberspace and its value chains (Kohl, 2017).

Making matters worse, the underlying structure itself is exceptionally technologically and organizationally difficult to secure when the national STES is largely unprotected and fully open to the rest of the world’s networks – across conflicting national legal systems, network controls and architectures, and cultural-cognitive presumptions. Any civil society seeking to defend its own national cyberspace faces a diversity of technological and proprietary challenges in orchestrating security at any level much greater than would otherwise have happened, had the original internet stayed largely within national borders and legal regimes (Powers & Jablonski, 2015). The overwhelming scale and variety of malignant cybered challenges – especially those by authoritarian states, their corporate state-champion proxies, and the huge state-encouraged criminal classes (in the case of Russia) – have overmatched the woefully out of date and inadequate defence tool chests of the formerly dominant civil societies.

For the first time in their collective history, the democratic allies do not have the proper mix in cyber power for defence and thus encourage the deepening of cybered conflict as adversaries experiment and learn what can be harmed at will. These adversaries can remotely remove or alter critical information and maintain backdoors for future actions from theft to destruction. Using the stolen IP or insider knowledge, they can bury, bribe, bully, or blackmail defending democratic corporate or political leaders. They can seem to legitimately displace the victim’s industry assets in the market while having behaved badly out of sight of most observers.

The result is the hollowing of the nation’s or group of nations’ abilities over time to respond or advance technologically and economically over time, eventually politically as well. The best way to destroy a democracy is by destroying its economy; the tolerance, transparency, and inter-citizen/institution trust vanishes rapidly, as demonstrated across Europe in the 1920s (Romer, 1992). While no state is a robust cyber power today, China has so far demonstrated the most strategic coherence in the use of its demographic and economic
scale to operate broadly and further its national security and economic interests. While the democratic states originating the internet struggle to even agree on cyber security, this rising authoritarian ‘anchor-state’ aggressively employs the five offense advantages through digitized proxies throughout the world. It succeeds in ubiquitously extracting massive amounts of STES data from other states, and is focused on acquiring the technology to rapidly process the data for foreknowledge and resource returns. It is well on its way to having a considerable head start in achieving robustness in cyber, and certainly its political leaders intend for it to be ‘the’ global cyber power (Inkster, 2018).

**Future China-dominated international system pur or moderated?**

**Existential challenge**

Today the most likely future global world order is a leaning-authoritarian China-centric international system. Chinese scale and strategic coherence dominance across all key fields of technology (DeNardis, 2012) and economy stand poised to determine the shared daily practices and flows of economic resources globally. A second future is possible and will take considerable work on the part of practitioners, private sectors, scholars, and leaders across allied civil society democratic nations. This alternate future is a multi-grouped, largely mixed, vaguely larger China-permeated international system with at least one major regionally resilient democratic subsystem jointly operated by a prosperous minority of unified civil society states who defend and transform, their collective cyberspace into a securable, generative, and advanced democratic IT substrate and market open for trade but not exploitation or abuse. If the latter emerges with the means to rescue a remnant of what is vanishing today in terms of the global governance regime (Nye, 2012), then cybered conflict is likely to continue but with less existential consequences for the small number of consolidated democracies in the world. The advance of the authoritarian STES model and technology-infused governance preferences are more likely to be blunted for decades, buying time for the defences of the civil society states, the securable rebuild and adaptive resilience of their democratic IT, and the democracy aspirations of much of the developing world to be strengthened.

The trends behind China’s rise to central player in the more likely future international system are to a large extent inherent given China’s scale in its singular demographic weight and commensurate economic influence due to market size. But it is also a function of the strategic coherence of the Chinese leaders in the CCP whose instructions are largely accepted by the wider society. At the end of the day, barring global catastrophe, it is inevitable that such a state would rise to the centre of the global system of states (Yuan, 2018). China’s actions to control their own internet and society resonate favourably with the wider developing world in which democracy – if it has taken root at all – is a shallow import easily adapted to underling authoritarian leaning, affective cultures (Chaihark and Bell, 2004). For China’s governing structure, the five-year plans are adapted to an outside world in which Chinese firms operate. These are more ambitious, economically realistic, and technologically and economically advancing than such plans proved for the former Soviet Union (Chan, 2018). As the nation progresses, adherence to the ambitious objectives in these plans is expected by all economic and government actors, and rewarded across industries and provinces (though both are skilled in obfuscation of concrete or objective results) (Zhang, 2016).

When several five-year plans in a row place telecommunications industrial dominance as a key objective, the desired strategic coherence of the state is expressed unequivocally. The goals are mirrored in the industrial scale projects and ambitions among competing commercial and political leaders. Even state champions have to comply. They push the seams
in the existing international rules of economic exchange in order to rise globally through determination and persistent presence. They exploit state subsidies, legal immunity, gaps in regulations across nations, and questionable business practices already well known in China (including the 4 Bs of bribery, bullying, blackmailing, and hostile buying) (Demchak, 2017). For the more important of these firms, this effort has succeeded so far. The Chinese telecommunications giant, Huawei, was not among the top seven telecommunications corporations in the world in 2004. In 2019, it is now the first, second, or third depending on the specific sector (Fan & Gao, 2016) – an unprecedented rise and some would argue impossible without bad behaviours en route (Bastone, 2019).

In many respects, the China-centric globe without the countervailing prosperous democratic civil society model is already apparent inside the country itself. Resources flow to the centre – Beijing or designated regional capital, and the economic value chains are expected to be designed to ensure that happens. In such a world, all decisions that matter globally or specifically – according to the leaders in Beijing – will flow through some central node, perhaps a compliant UN, with China’s right to primus inter pares if it chooses to sit at that discussion. China has a long history of ‘vassalization’ that, unlike the colonialization of Africa by the Victorian states, does not necessarily include regime change, but it does include an automatic veto and first bite at any apple if desired by Chinese representatives (Swanström, 2005; Cohen, 2006; Clarke, 2010). Given the ubiquity of the huge Chinese diaspora today, the coverage of those representatives will be extensive geographically. It will be strategically intense where Chinese national interests have been declared, including natural resources, especially energy and food, and advanced manufacturing (if it has not already been moved to China proper). Already Chinese leaders have shown a willingness to punish violators of their preferences across a myriad of issues relating to telecommunications, finance, space, and political speech deemed disrespectful by the Chinese regime.

Economic statecraft – especially coercive punishment for noncompliance – will be overt, pettier, and likely routinely more severe in the China-centric future. Many lower level decisionmakers representing the CCP will be given autonomy in, kudos for – and profit from – acting more vigorously in defence of Chinese interests (Blanchard & Ripsman, 2003; Blackwill & Harris, 2016; Norris, 2016). Overreach will happen but, since the critical political and senior economic leaders in the vassalized states’ STESs will be in the Chinese-sphere of strong influence, resisting states will have difficulty mounting a credible unified political or economic response short of war. With no unfettered media, the grievances will be buried in government automated censorship or agencies, possibly also with the bodies of those who spoke to loudly or attempted to organize resistance. In short, major parts of the world are likely to present as quieter in global media terms, calmer in political struggles, more controlled in social behaviours, and more generally compliant with central preferences from Chinese representatives across sectors of interest in each state (McKune & Ahmed, 2018). What civil society would term routine ‘bad’ business and political practices such as nepotism, corruption, usurpation of rights, arbitrary search, confiscation, and seizure, cro-monyism, inflated or false reporting, deception, and brutal political control will mark the intra and interstate behaviours in the China-centric system lacking a democratic countervailing influence (Hannas, Mulvenon & Puglisi, 2013; Bradley, 2015; Haddad, 2016; Wong et al., 2017; Wang, 2017). There is a second possibility, however, of a moderating, even possibly mitigating global influence role played by a minority community of democracies. For this future to occur, this group must actively ensure that its members cannot be peeled apart and individually economically, technologically, or regionally vassalized by state-sponsored bullying, bribing, blackmailing, buying, charm offensives, or deception. The community must
trade with, operate in, and provide the international system with an alternative model of governance, security, and values. The consolidated democratic civil societies – despite being roughly 10% of the global population – could ensure their own wellbeing and survival by organizing collectively into a rough demographic peer to China and act with strategic coherence in key technological and economic areas. Especially critical would be institutionalizing the process of securing the cyberspace substrate by transforming it, and defending thereby the economic wellbeing dependent upon it.

Today western states’ leaders are for the most part finally beginning to recognize the long-term national security implications of the true magnitude of those cyber-related economic losses. Only now has the United States formally included the defence of its economy as a national security mission for its key cyber unit. Only now has it, along with France most recently, recognized that defending its economic actors may require what was previously taken off the response table – persistently proactive cyber actions against foreign perpetrators. Individual national steps are, however, not enough to counter the scale of the assaults nor the urgency of the situation.

For the democratic civil societies, this deepening cybered conflict along with the rise of a more aggressive China now imposes an existential choice – hang together or most assuredly be separately, economically-technologically vassalized, and eventually marginalized globally. Needed is a more collective and comprehensively operational response for defending civil society powers to amass the countervailing systemic STESs foreknowledge and the scale of resources required to mitigate, neutralize, recover from, and innovate beyond the uncertainties and insecurities of the current shoddy cyberspace. Only by coalescing as a decidedly democratic force with 900 plus million people, operationally joined across key telecommunications and IT capital goods (as well as energy and finance) aspects of their interlaced socio-technical-economic systems can the minority community of consolidated democratic civil societies survive. This community must coalesce the requisite scale and strategic coherence necessary to have a reasonable chance of being recognizable prosperous and defensible democracies in 60–80 years.

Collective response essential in cybered conflict and needs research and action – CORA

Irrespective of how the future develops, and whatever cybered conflict is called, it will be a continuing source of uncertainty and insecurity for all states. For states that intend to survive as consolidated democracies, however, this conflict will be particularly hard unless the underlying substrate so poorly built is itself transformed into something defensible for democratic values and their value chains (Mallery correspondence, 2012–2019) These democracies have to alter the playing field of this kind of battle in order to make it less productive for adversaries. Whatever mechanism is created to ensure the survival of robust democracies in the coming system, the construction must begin soon to the narrative and the institutional structures in place and able to defend the intertwined STESs and their economic vitality.

First and foremost, the fractious advanced democracies will have to combine to build actionable scale and a collective strategic coherence. Given the rapidly growing losses in their economic wellbeing, these nations need to buy time for the R&D blitz needed to transform the shared cyberspace substrate underlying their allied environments into something defensible for democratic values and value chains, and still generative of economic and innovation advance. One particular mechanism – a ‘cyber operational resilience alliance’ (CORA) – offers both (Demchak, 2019). The alliance would link the telecommunications industries
Cybered conflict, hybrid war

with the IT capital goods industries with their respective governments and militaries in an operational, joined effort that defends all the allies and their cyber-dependent economic actors. In return for their commitment to the overarching goal of collective reduction in insecurity, the IT capital goods sectors are provided a 900+ million strong, single democratic community market free of authoritarian proxy corporate subversion, hostile or coerced ownership, or tainted business competition with no reliable legal protection. The CORA would make the joint, existing cyberspace substrate as secure as possible for now while coalescing the collective and massive investment across universities, industries, and governments needed for its transformation and the survival of civil society economies and values over the long time.

Considerable consensus, funded widespread research, and multi-sector accommodation and implementation are critical now. Whatever specific forms this conflict takes at any given moment, it will be a losing situation for those states who do not adapt and seek to change the terms of the conflict in their favour. The coming world advantages those actors able to obtain foreknowledge and resources at scale to develop robust cyber power and impose their preferences on others across the connectivity, content, and cognition elements of whatever technologies compose cyberspace in the future. China has already demonstrated what may be gained by having strategic coherence and scale; its role in this future world varies from central node to nearly central node in demographic, technological, and economic terms, barring global catastrophes. How that future resolves for democracy as a desired governance model and for democracies in the future as prosperous, defensible, and tolerant transparent societies greatly depends now on the research and actions by the scholars, practitioners, and leaders of those nations today.

Developing the collective action scale and strategic coherence of a CORA will take rethinking current assumptions about the international system, economic models, and the role of advancing technologies and complexity in national STES. This chapter takes both a deep and wide-angle view as a call for action by young scholars, experienced practitioners, and senior leaders in public and private sectors. It is time to integrate what we know not just from the past 10 years but also from systemic approaches in social, technical, and economic disciplines. Cyberspace – especially the heightened possibility of acquiring foreknowledge in unprecedented amounts, validity, and ease with impunity – has changed the conditions of human contestation, even if not the motives. Authoritarian states today use different terms than their counterparts in the democracies – such as hybrid war or informatization war, but they are widely experimenting and pushing aside the liberal internationalist assumptions of the post-Cold War era and the realist bipolar models from the Cold War period. It is time to discard much of the dated presumptions set in cement during those highly artificial circumstances of the US-USSR Cold War. New theories are needed in fields of economics, war, comparative social science, security studies, complex adaptive systems, politics, largescale technology systems, international relations, and the emerging field of STES studies in order to ensure the survival of democracy in the rising cybered and post-western global reality.

References


Chan, E. (2018) The ‘made in China 2025’ plan aims to break China’s reliance on foreign technology and pull its hi-tech industries up to western levels. *South China Morning Post* (September 10).


Cybered conflict, hybrid war


Hathaway, M. (2013) *Cyber Readiness Index 1.0*. Great Falls, Hathaway Global Strategies LLC.


Riley, K. et al. (2005) State and Local Intelligence in the War on Terrorism. Santa Monica, Rand Corporation.
Thomson, I. (2019) Spyware sneaks into ‘million-ish’ asus pcs via poisoned software updates says kaspersky – hackers were interested in 600 or so targets, it is claimed. The Register Online. Available from: www.theregister.co.uk/2019/03/25/asus_software_update_utility_backdoor/ [accessed 9 June 2019].
Cybered conflict, hybrid war


