Achieving Systemic Resilience in a Great Systems Conflict Era

Coalescing against Cyber, Pandemic, and Adversary Threats

Chris Demchak

ABSTRACT

A converging trifecta of national disruptive threats – pandemic, cyber attacks, and a rising authoritarian China – is draining the wealth, political harmony, and international influence of today's consolidated democracies. The result is a more palpably apparent decline in the likely future of democracy as the preferred regime alternative world-wide. The collective dismay and frustration may, however, offer a rarely open door for better postures for democracies in facing a more, not less, turbulent future. This article makes three arguments about a new and more accurate characterization of the coming world as Great Systems Conflict, a list of minimal must-do actions for systemic resilience, and the collective structures critical for resilient democracies over the long-term. The article ends with a discussion of two examples of structures meant to build cybered resilience for allied national systems—domestically in the National Cyber Security Centre equivalents and across consolidated democracies in a Cyber Operational Resilience Alliance.

Today, consolidated democracies face a convergence of three major systemic threats: a raging viral pandemic, an ever-growing tsunami of malicious cyber-attacks, and the inexorable rise of a large scale, strategically ambitious, authoritarian adversary. The cumulative effects of these three threats at the same time are draining wealth, political consensus, and global influence, with increasingly poor long-term prospects for democracy as a dominant regime alternative worldwide. Consolidated democracies thus far have demonstrated a limited community response. As individual national socio-technical-economic systems (STES), each country—both democratic and authoritarian ones—varies in their internal responses to adverse health, cyber, or adversary threats, but none has demonstrated the ability to be resilient to all three systemic threats. The growing

With degrees in engineering, economics, and comparative complex organization systems/political science, **Dr. Chris C. Demchak** is the US Naval War College's Grace M. Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber and Innovation Policy Institute (CIPI) – formerly the Center for Cyber Conflict Studies (C3S) which she co-founded and directed. Her research and many publications address global cyberspace as a globally shared, complex, insecure 'substrate' underlying the critical organizations of digitized societies, creating 'cybered conflict' and a resulting, rising 'Cyber Westphalia' of sovereign competitive complex socio-technical-economic systems (STESs), and inducing an urgent survival need for a 'Cyber Operational Resilience Alliance' (CORA) among advanced democratic allies. Demchak takes a systemic approach in focusing on emergent structures, comparative institutional evolution, adversary/defensive use of systemic cybered tools and artificial intelligence, virtual worlds/gaming for operationalized organizational learning, and in modeling systemic resilience ('cybered conflict model') against normal or adversary imposed surprises that disrupt or disable largescale national systems.

number, volume, and sophistication of malicious cyber-attacks reduces consolidated democracies' GDP growth by 1-2%, moving some into negative growth for 2020.[1] Social tolerance, trust, and transparency that distinguish democracies have also palpably declined. While one highlights cyber and state-level adversaries here, the analysis and recommendations also apply to an inability to respond systemically, except negatively, to pandemics. Democracy is at stake in national responses to all three threat streams. As nations bar movements to stall infections, they further decrease the already declining openness of internal and international systems epitomizing democracy and the international liberal economic system.

When the sources of frightening systemic uncertainty converge into a triple threat—a trifecta for short—to overwhelm both the warning time and the resources to respond across most open societies, resilience comes back into policy circles as a popular word. Whether the threats come from increasingly ubiquitous debilitating viruses, from disruptive cyber maliciousness or shoddy programming, or from deliberate campaigns by multiple adversaries, it is well recognized that only a strategy of resilience—properly understood—can structure the necessary narrative and practices of the targeted system's internal responses. The goal is that uncertainty from outside is manageable and insecurity on the inside is minimal. Compounding this challenge, unfortunately, leaders too quickly lose interest in providing for the costs, time, change in behaviors, and updated narratives essential to achieve long-term resilience. The work goes out of fashion as soon as the threat of the moment has passed, whether it is war, a massive breach, or even a pandemic that paradoxically does not kill enough people to be memorable.[2]

Today's convergent trifecta of nationally disruptive threats may offer a rarely open door for collective change, resilience, and better postures for democracies facing a more, not less, turbulent future. Taking

this unusual opportunity will require a new and more accurate characterization of the coming world as "Global Systems Conflict," a list of minimal must-do actions for systemic resilience, and the creation of collective structures critical for resilient democracies over the long term. With that goal of capitalizing on this opening to possibly make a different future path for the world's relatively small community of consolidated democracies, this article makes the following three arguments.

First, emerging as the backdrop to future vitality threats for democracies is "Great Systems Conflict" rather than the more traditional "Great Power Competition." Its global ubiquity will force collective whole of society resilience to become a primary objective of national security and economic—as well as health and well-being—strategies in the not distant future across like-minded democracies. Second, resilience is an ongoing organization-driven process, not a static achievement, with an empirically identified set of minimum requirements for large-scale, complex socio-technical-economic systems (STES) such as nations. Third, resilience requires strategically coherent structures to manage integration across these requirements in response to pandemics, cyber or its offspring in AI/ML, and national autonomy threats. These structures can be merely dampeners—the speed bumps or near-term barriers—holding off threats for the short term, or they can be the strategic introduction of "slack in time," furthering the resilience of the overarching system. The article ends with a discussion of two such structures meant to build cybered resilience in Great Systems Conflict for allied national systems—the National Cyber Security Centre and the Cyber Operational Resilience Alliance. These structures can be blended with, or mirrored into, equivalent structures for pandemic resilience as well.

I. "GREAT SYSTEMS CONFLICT" IS THE NEW "GREAT POWER COMPETITION"

Today, the US and its allies are in a "Great Systems Conflict": a digitized interconnected struggle between national socio-technical-economic systems in terms of their ability to withstand large-scale disruptive threats, whether from relentless adversaries like China, from the massive cyber bad actor community, or the enormous scale of poor programming that undergirds cyberspace globally. Even pandemics pit state systems versus other state systems in terms of their ability to channel incoming infection hosts, block internal transmission, vaccinate appropriately, or accommodate the health and economic disruptions of thousands of extremely sick and infectious people. When the latter health crisis occurs while intelligent adversaries or bad actors are also systemically unchecked, then a threat trifecta of assaults can put nations on their knees in ways that throughout history only military contests in war or sudden global climate eruptions could achieve.[3]

To better understand our needs going forward, we must update the narrative to reflect the challenges now facing democratic states. Systemic assaults from multiple domains or sectors require systemic readiness and agility not required nor demonstrated in history's "Great Power" eras. It is time to retire that newly resuscitated term before it leads us away from a clear-eyed understanding of the current and coming world.[4] In fairness, the current popularity of

the term "Great Power Competition" (GPC) has served its purpose well. Over the past few years, the rising use of the phrase efficiently highlighted a changing world system and alerted those asleep at the wheel or unwilling to let go of the US global dominance *zeitgeist* to acknowledge a new global reality. The hook worked—policymakers are listening.[5] Now we need to jettison it and adopt more accurate language and interpretation that stimulates, rather than stultifies, strategic thinking.

What this convergence of threats demands of each nation is not the same as was required of geographic sovereign powers one hundred or even forty years ago. As John Mearsheimer pointed out in 1991, the loss of the bipolar world would lead to struggles for hegemony rather than harmony.[6] In the coming eras, opponents are less likely to leap to the edifying clarity of armed clashes in war than to attempt to achieve the same goal across the defender's entire internal socio-technical-economic system through digital, economic, and social means. China recognizes this new reality, but advanced democracies are struggling to adjust, whether out of complacence or confusion. Hence, it helps little to keep telling ourselves that we face something we have seen before, and it is particularly disabling when the trifecta of systemic threats is well underway. What one calls something—especially if it has resonance with the past—heavily channels what one pays attention to, interprets, and does. Mislabeling can be strategically misleading and a prelude to defeat.[7] For example, it was not by accident that the British pre-WWI called their new armored vehicle a tank. It looked like a water tank and so the name served as a good disguise. But it also led them to think of the tank as an infantry support vehicle rather than an assault vehicle, a blindness Germany exploited in World War II.[8]

Ultimately, to continue to use the "Great Power Competition" label tells us little about how to defend an entire socio-technical-economic system (STES) where adversaries can easily poke thousands of fingers into all of democratic nations' socio-technical-economic pies.[9] Today's struggles do not begin, nor will they continue, in the same dance around the geographies of armed territorial borders that marked the last century's Great Power competitions and nearly all of the previous ones as well.[10] This still emergent century is not characterized by a multipolar tumble of shifting alliances in "a multipolar system, a general disregard for rule-based constraints on behavior, and dominantly political-military forms of rivalry."[11] While it seems to create a consensus rhetorically, the term itself has too much historical baggage.[12] Bad analogies lead to bad strategies.[13]

Such imprecision is not just misaligned with the deeply digitized world around us; it is also strategically dangerous.[14] The term encourages a rough equivalence in assessments of large state actors as though any nation at the top—irrespective of socio-technical-economic scale and strategic cohesion—could take the global lead at any point. It encourages ignoring the future path channeling effects of Russia's constant near-term strategy of disrupting and obstructing the US and EU. It strengthens a false view of equivalence between Russia's goals and China's longer term, systems-versus-systems strategy to supplant the US. Strategic mischaracterizations

not only lead to missteps in general with each nation. They can also encourage actions that "could end up driving Xi and Putin into each other's arms," creating a combination that dramatically increases the strategic scale and complexity of the national security threats.[15]

A "Great Systems Conflict" (GSC) emerges when large-scale nations engage in adversarial operations to weaken opponents across the multiple, complex, critical sectors within and among nations without the clarity of sides and actions in declared, kinetic wars.[16] It is the horizontal expansion to all national domains of the cybered conflict spectrum between peace and war. In this GSC, no system is off the table a priori. This free-for-all-who-can taint is especially present if the malicious usage can be skillfully obscured for considerable time in, perhaps, the hijacking of data traffic by Chinese telecommunications companies across the internet exchange points of democratic nations' cities[17] or the corruption of critical network management software updates across the Fortune 500 firms as happened with the 2020 SolarWinds Russian campaign.[18] Nations involved in GSC cannot assume any opportunity to enhance disruption will be neglected, even if the sources seem natural in the form of complex systems surprises such as the failure of Boeing's 737-Max aircraft[19] or biological in the form of 2020 pandemic outbreaks. Strategically navigating that multi-domain maze of contestation does indeed include the exquisite targeting of adversaries' offensive elements to blunt some campaigns. However, above all, it requires withstanding the assaults of millions of hits per hour into and across the integrated digitized systems that keep us viable—our economy, critical infrastructure, and democratic institutions.

It is high time to move to this more accurate term of "Great Systems Conflict." The more tied to current reality the explanation, the dominant narrative, and its term of art is, the more likely the nation's community elites and organizations are to recognize their collective security as a need and be open to discussing the benefits and negotiating obligations in systemic resilience. People cannot get behind a strategy that describes a world they do not see. Characterizing this century's existential competition as a struggle between "Great Powers" seriously departs from the world inhabited by the leaders of our businesses, the civil society community, or the citizenry at large. Defense sounds like a game of kings best left to the political leaders at the top, with no responsibility, obligation, or benefit to anyone else short of war. Systems-versus-systems conflict requires citizen buy-in over the long term to succeed.

The future will be marked by systems-versus-systems manipulation by bad actors and adversaries. Only the transformation of the underlying shoddy cyber substrate, as well as health and economic infrastructures, will truly prepare democracies need to get fully engaged in this mission. As societies become more complex with cyber's offspring such as AI, especially neural net learning, robotics, and other combinatorial cross-tech advances in bio-sciences, nano, and other advances in the sciences, surprise becomes more common. Attack surfaces massively increase, and adversaries become more emboldened, skilled, and ubiquitous. While disrupting adversary campaigns to signal displeasure or stop harm is

important, "defend forward" operations such as those conducted by U.S. Cyber Command (USCYBERCOM), cannot alone match the scale of inputs of the wider digital environment without wider support from allies and the private sector.[20] When socio-technical-economic systems are contesting each other within the entire space of their myriad interactions, systemic resilience becomes the priority strategic imperative.[21]

II. RESILIENCE'S CHALLENGE[22] FOR SOCIO-TECHNICAL-ECONOMIC SYSTEMS

Resilience is a complex system's capacity to acceptably anticipate, accommodate, and innovate beyond urgent, disruptive, deleterious surprises. A resilient system demonstrates "the capacity for collective action in the face of unexpected extreme events...[involving] processes of sensemaking and creative problem solving...in complex, social systems...[and] actions that range from improvisation to innovation under urgent conditions."[23] This definition comes from scholars with years of experience studying resilient systems. Beyond the experts and those practitioners directly engaged in making systems resilient, however, the word has many—one could argue too many—variations in common understandings.

What we know about resilience comes from a handful of literatures focused on biological systems, on crisis management in societies or businesses, and on technological systems crippled by normal accidents or deliberate attacks. The first highlights long-term survival of the whole community or species over individuals; the latter two, on the restoration of the damaged system under review. When abstracted away from the details into a view of parametric stimulus-responses, accommodating adjustments rippling through connections, and finally stabilizing structures, these literatures point to six elements common to all successful resilience stories.

1. **Slack-in-time** through separation to delay the incursions of threat and give warning to decomposable, self-sustaining operational units.
2. **Redundancy-in-knowledge** to give surprised actors or systems the precisely required knowledge.
3. **Discovery-trial-and-error-learning (DTEL)** by each of all decomposable units to foresee and resource for surprise.
4. **Collective sensemaking** before, during, and after across all decomposable units.
5. **Collective proactive action arrangements** and maintenance of capacity to act.
6. **Collective frequent whole-of-system practice** of all responses as group DTEL.[24]

These six elements are a minimal list of requirements and are listed in logical order according to their clear expression in empirical cases and to the scale and number of the systems—usually organizations, enterprises, government agencies, or communities—involved. Another way to present the list is as a rough approximation of what comes first in human organizational thinking. Faced with huge and usually looming physical threats, humans run to barricade

themselves to separate for some *slack in time* in order to do some *sensemaking* among each other. Once temporarily protected, they may do some preplanning and envisioning to *mentally think through* what they anticipate is coming next and decide *what actions must be performed* by whom, when, and where. They gather *redundant stores* of resources to place them in the locations their *collective vision* of the immediate future indicates as most appropriate for the survival of the entire system.

Recent years have shown this process playing out in fragments across all three threat streams of the trifecta, but rarely are the six requirements fully met by any large complex system throughout history. They are difficult to achieve as the size of the socio-technical-system at risk grows, and as the volume, diversity, harm potential, frequency, and opaqueness of threats balloon as well. The grand challenge of designing a resilient system rests in structuring that volume and simultaneity of complex resilience calculations and actions continuously across the nation's social, technical, and economic domestic ecosystems toward greater achievement of, and integration over, all six requirements. Furthermore, today it is also necessary to accommodate some key variations of the resilience challenge across all three threat streams of the trifecta currently assaulting democracies.

For the vast tsunami of bad actors using cyber, for example, a key and framing distinction is how relatively easy and cheap it still is to use the five offense advantages built into cyberspace by the shoddy coding of the original creators of the Internet. Cybered criminal and adversary actors continue to use massive scale of botnets as attack organizations, and benefit routinely from unparalleled digitized proximity, as well as endless choices in precision of weapons, deception in tools chosen, and opaqueness of one's true origins. All remain readily available in forming attacks or campaigns against distant strangers in foreign socio-technical-economic systems one or many at a time.[25] Despite everything laid on top of it for security, the underlying, global cybered substrate continues to be built with insecurity in the confidentiality, integrity, availability, nonrepudiation, and transparency of data, not for the resilience of the nations relying on it.[26]

For pandemics, the list of framing distinctions is even longer. It includes generalized food insecurity leading to the introduction of wildlife viruses into the human food chain, wealth disparities linked globally through international transport of people, insects, plants, and illegal trades in protected or undesirable biological specimens, and wide disparities in national policies, capacity, and attention to biological health of domestic populations. Across history, there have been few pandemics that were predicted before they manifested and actively contained in humans. The events of 2020 and the SARS-COV-2 epidemic suggest in cruel and costly terms how little systemic resilience to this threat stream there is internationally.[27]

State-level adversaries pose distinctive challenges to achieving resilience in terms of their deliberate use of demographic and economic scale strengths and their intelligent deployment of strategic coherence. While a virus mutates automatically, and the cyber mass of criminal and

malicious actors moves organically away from hard problems in response to adequate systemic resilience, adversary states have strategic interests that do not easily change. They and their proxies are often relentless in diverse multi-domain, multi-sector, and multi-target campaigns. To respond to the adversary's complex systems surprise and the malicious mass of bad actors, defenders will need resilience as the first and primary defense. It is important to note, however, that resilience needs a more pointed response such as the USCYBERCOM's "forward defense" implementation of its "persistent engagement" strategy, to provide legal, coercive options that reinforce defensive deterrence.[28]

Across all three of these streams then, systemic resilience programs will have to dismantle the five offense advantages of cyber, and effectively orchestrate a coordination of national policies in health, food, and monitoring of viral spread through illegal trade in wildlife at a minimum. Plus, systemic resilience strategies help democracies match the scale and strategic coherence of the major adversaries in order to deny and disrupt adversary campaigns. The first response invariably is intended to generate slack-in-time.

A. Always the First Step: Separators to Build Slack against Threats

Resilience structures are created by a separation architecture, i.e., varieties of openness within the system that allow unfiltered inputs, intended to provide slack-in-time, the first resilience requirement. Empirically, this structuring response is as old as human society when the first clans sought to improve survival through barricades for defense and the division of labor whether in acquisition of food or in capacity for fighting.[29] Those with one job were separately trained from those with other jobs, and the clan itself. Many modern concepts capture these designs, parsing elements of STES, for example, division of labor in organizations, parent-child objects in software design and self-contained subsystems in engineering, or enterprise product divisions or regional markets in economics. Everywhere separation of elements is used to control inputs that cannot be processed as quickly, efficiently, profitably, safely, and/or securely if left as a completely open input stream.

It feels natural to wall oneself off from threats; reduced internal disruption means reduced uncertainty and the separation offers more time for a response to develop. John Kenneth Galbraith, a seminal author on information systems in organization theory, argued this response was not just instinctive. It was also the only choice if the internal systems could not be made to process overwhelming inputs of information faster than the data came in.[30] For a similar reason, Thompson argued organizations were always somewhat open to surprises from their environment.[31] The recommendation to separate clusters for more response time and increased ability to monitor inputs is found in many literatures including engineering resilience research. The well-honed response is to design an overly complex system in a way that limits failures to certain sections or components, allowing for more rapid isolation and diagnosis of a smaller set of candidate components which may then more readily be corrected.[32] Modern secure cyber architectures also embed separation in forms from micro-segmentation[33] to con-

tainers in clouds. The goal is to slow the transmission of error from external sources to dampen the internal amplitude of the sequence of failures across linked systems and give the defenders or maintainers more time to respond appropriately.[34]

Today's pandemic also shows this instinctive reach for slack-in-time through quarantines and travel bans. Pandemic pods are a particular expression of ad hoc and bottom-up separation choices, usually with rules—much like in organizations—that determine who is in or out, what are acceptable levels of out-of-pod activities, and how to communicate threats, errors, or reassurance.[35]

Slack, however attractive as the first and usually ad hoc response, is only one requirement. All too often, separating from the threat is all that is accomplished in a system, and generally this is short in time, reach, or funding, and usually abandoned or severely reduced when the crisis has passed. Without an integrated systemic response addressing all six resilience requirements, each new major threat event continues to hollow out the nation's future well-being.

B. Second through Sixth Requirements Often Neglected

Slack architectures provide the structures for potential resilience, but this can only buy time. Their mechanisms of separation define the edges of components, organizations, and even borders for states, but cannot provide a missing narrative of cohesion that fosters consensus and the creation of "statecraft"[36] for action across a nation.[37] The use of slack cannot compensate for resilience shortcomings that currently are found across all three threat streams. For example, there continues to be a lack of a consistent narrative on the pandemic despite mounting deaths.[38] Slack responses cannot alone assure the necessary local and collective discovery-trial-and-error-learning (DTEL) processes that would have helped the US in its 2020 pandemic response. Other shortcomings in resilience are common as well. Highly localized or deliberately underfunded redundancy in knowledge restricts urgent, real-time updates to only a few or forms echo chambers in which adversary disinformation can more easily demobilize or falsely mobilize citizens.[39] DTEL is found only in many small one-off or highly proprietary or classified exercises or simulations, dramatically limiting the learning to small groups.

Collective sensemaking and action arrangements are similarly confined to small, trusted groups or leading industries. The larger the group, the more sensemaking and action preparation become exercises in checking-the-box compliance. Finally, any collective whole-of-system exercises to create whole group DTEL tend to be held by governments or for government agencies with private sector observers, with results classified away from the rest of the society and possible allies. Crucial players in a whole-of-system defense, especially in cyber (e.g., the nation's IT-related private sector), are left out of strategic deliberations, incentives, and commitments. It is worth asking why recent successes in election defense by US agencies have not been immediately pivoted to the defense of the healthcare system wracked by ransomware and IP exploitation intrusions into vaccine research during a pandemic.[40] The answer is clearly a lack of a resilience mindset and appropriate structures.

III. COHERENT STRUCTURE FOR INTEGRATION ACROSS RESILIENCE REQUIREMENTS

Creating structures for long-term resilience means making and empowering organizations. All systems contain structures that divide the labor or contribution to the whole, assemblages of technical components, and transactional processes among elements of the system. This division of labor is found in organizations separated for a collective and strategic purpose, usually to accomplish something that would otherwise not be so timely, cost-effective, or possible without the overall organizational structure.[41] An organization is needed to provide strategic coherence in resilience, placing the dampeners throughout the system proactively according to sensemaking needs and action arrangements as adjusted by local and collective DTEL.

A strategically placed and correctly scaled organization to nurture and ensure the proper integration for resilience against threat streams has been repeatedly recommended in the past. Today, however, the revival of interest in resilience and the associated suggestion that the instinctive reach for slack be channeled through an integrating organization is more than a rehash of an old platitude. In the age of Great Systems Conflict, the lack of this integrating mechanism has long-term existential consequences. The turbulence and vigor of GSC will not decline, nor will COVID-19 be the century's final pandemic. A fragmented, ad hoc, siloed, non-resilient response by a democratic STES paves the way for local and global decline in cyber, health, and defensive capacity.

Governing the system containing the assets at risk in GSC helps enormously in defense because the members can agree to reshuffle their internal architecture to direct more efforts in making a higher work factor[42] for adversaries. Or they can agree to collectively reduce complex systems' surprises by breaking down the whole into parts able to defend more readily and degrade less disruptively.[43] The more members of the system at risk agree on their sensemaking narrative and accept that their capacities (DTEL and their redundancy in knowledge) can and will be used to forestall, deny, or work through threat assaults, the more systems will be organized, strategically coherent, and able to operate through threat streams. For this to happen, a strategic and managing layer needs to be structured to manage slack placement, redundancy in knowledge development, local and collective DTEL, and the collective agreements in narrative and commitments to action.

Furthermore, any strategic organization dedicated to systemic resilience needs to be scaled to the size of the socio-technical-economic systems under assault and to the character of threat sources. For example, large businesses and nations have internal boundaries that dampen viral or cyber movement and naturally create slack, enhancing their short-term defense against predators who aim to decimate or cripple the community. However, that size may not prevent the harm if the integration of transactions is so rapid that all elements are infected, affected, or disrupted nearly simultaneously.

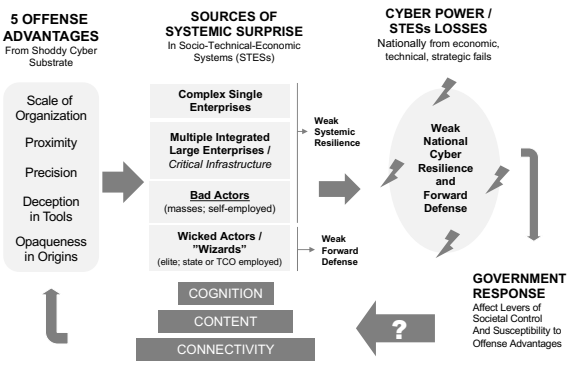
Several nations have already provided organizational experiments in domestic strategic resilience against cyber assaults and adversary campaigns. These exemplars also suggest that, if not already in place or under development, equivalents are necessary for resilience in pandemics.

A. Natural Experiments Suggest Anchor Organizations Critical to Internal Resilience across Complex STESs

Within each national socio-technical-economic system, defense of the entire system—the country—is traditionally left to the government. This makes rough sense in that only the government in a democracy has, in principle, the electorate's mandate to make decisions on their behalf and therefore the legitimacy to enforce those judgements in defeating attacking enemies. However, viruses are not subject to electoral preferences, and, up to now, neither has the cyberspace substrate been subject to many governance intrusions in open democracies. So far, consolidated democratic governments have floundered while trying to integrate responses to cyber assaults. They are highly variable in response to pandemics and too narrow in their reactions to adversary campaigns. The next section will address cyber assaults specifically, with the proviso that the resilience organization discussed here has application for both pandemics and adversaries.

Since its inception, cyberspace has been frequently promoted as a special technology whose generative capacity will be destroyed for the whole society, even the world, if governments attempt to regulate it in any way.[44] The consequences have been systemically dismaying and costly. Underlying both the cyber and adversary campaign threat streams is a cybered conflict cycle of systemic harm. It began in the 1990s when the US IT capital goods industry created a highly insecure cyberspace substrate that then spread globally—with five embedded offense advantages sent to all bad actors, including states. Democratic government responses have been largely fragmented, derailed by knowledge inadequacies, ownership challenges, and strategic incoherence.[45] Figure 1 shows this currently endless cycle of malicious use of offense advantages enhancing systemic surprise and poor national systemic resilience with narrowly focused responses by democratic governments unwilling to act to impede their commercial IT producers, thus ensuring the cycle continues.

Figure 1. Cybered Conflict Endless Cycle of Poor Resilience[46]



The lesson of the past ten years in cyber security and national defense is that leaving the national STES to self-organize a resilience-integrating anchor organization is a fool's errand. Because individual enterprise leaders lack a collective narrative regarding the seriousness of experiences so far, no sufficiently large subgroup has formed to lobby the government for knowledge or action on behalf of the entire system. Governments matter to systemic resilience and must be directly involved in the creation of any organizations designed to break this cycle, integrating the efforts of the whole STES across the six requirements for any threat stream.[47]

Two experiments in creating an anchor organization for an entire nation in its defense against cybered conflict onslaughts are worthy of mention and future study as they evolve. The first is the United Kingdom's National Cyber Security Centre (NCSC),[48] and the second is Israel's National Cyber Directorate (INCD).[49] Each occupies a pivotal position in governance and in access to knowledge. Each already demonstrates some success in influencing the national narrative about cyber security across networks and in the development of cyber's offspring in AI/ML and autonomous technologies. Each also has become the central anchoring point for private sector actors to interact with government points of contact on cyber help, regulations, or threat campaigns. Neither is the perfect solution, but each presents a major step forward in developing strategic coherence for the entire system.[50]

Other NCSC close equivalents are worthy of further study. Although they are at different levels of collective sensemaking, two examples of government's relationship with the private sector are Netherland's NCSC[51] and France's ANSSI.[52] Most of the consolidated democracies, however, struggle with fragmented strategic actors in government and limited private sector involvement in collective cyber sensemaking, action agreements and support, and most forms of DTEL needed for system resilience.[53] The US shows particular difficulty, thinking in silos of narratives as it has limited private sector involvement save as technology or telecommunications providers. There is no unifying narrative and no single national organization capable of producing a compelling story or the integration required for national resilience. As one of the largest of the beleaguered democracies, the US provides a particularly unfortunate example for the entire community.

At the small end of the demographic scale is Estonia, one of the few democracies to have experienced a potentially devastating cyber-attack by a large-scale adversary and to have innovated through and beyond it. Estonia offers a benchmark for what might be possible in larger democracies. Kohler argues Estonia combines strategic coherence, "just-do-it innovation, commitment, and frugality (it fulfills the NATO target of spending two per cent of GDP on defense), collective defense (it consistently advocates for enhanced cooperation in cybersecurity and a holds strong stance on deterrence), and a persistent norm entrepreneur for the like-minded."[54] Innovative examples from small states can be quite instructive. If an innovation in structures or policies or socio-technical-economic whole-of-society integration

works in relatively small Estonia, larger states have a reasonable chance that this innovation will work at scale for their STES. If the experiment does not work in the smaller state with its relative advantages in cohesion, there is little chance it will work for larger states. Innovative responses among small states are thus well worth considering for a scaled-up experiment in the more fragmented systems. Both Estonia and Israel serve this purpose as innovation sandboxes for experiments in better designs of national resilience.

Having an anchor organization integrating all six requirements into a narrative and normalization of shared national practices is critical for domestic systemic resilience. It is also necessary for the like-minded to be able to develop and build on for a larger collective and resilient systemic defense against the relentless assaults of major adversaries, specifically China.

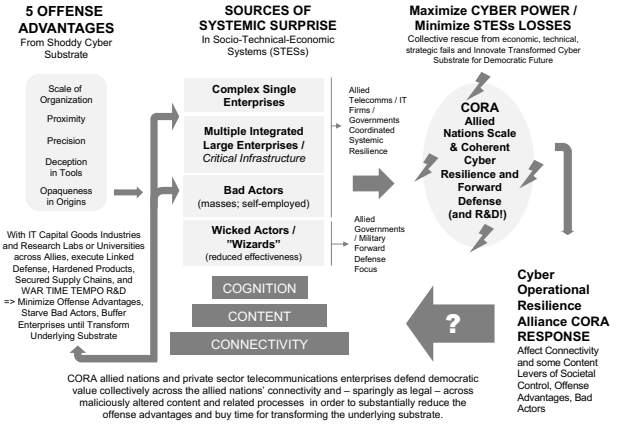
B. Cyber Operational Resilience Alliance (CORA) for Narrative Consensus and Strategic Coherence at Scale

> "The point here is not to change the Chinese government or dismember China or something. The point is rather to say, 'Look, we've got a position of power along with people who have similar interests to ours, [and] you can't dictate to all of us.'"[55]

If nations can rely on allies for the sharing of difficult requirements such as redundancy of knowledge, the imposition of slack at critical exchange junctures, and the resources for discovery-trial-and-error-learning (DTEL), no single nation faces the adversary alone. The resilience of a nation alone can easily fail facing an ambitious major adversary's scale and strategic coherence brought to bear from thousands of sources given its global reach. The like-minded defenders need to combine and thus scale up to achieve peer power stature vis-à-vis the adversary. The group needs to manifest strategic coherence in the actions they take to repel and innovate beyond the adversary's campaigns. If the resilience requirements are absorbed and instantiated across the defenders, the collective scale enlarges the resilience options across all the participant systems.

A structure is needed to ensure allies would collectively be effective. A Cyber Operational Resilience Alliance (CORA) is one way to engage in the collective sensemaking, collective proactive action agreements, mutual support, and group DTEL to continuously improve on all the interrelated practices, knowledge accumulation, and updated narrative. Figure 2 shows how this collective institutionalization can disrupt the cybered conflict cycle of harm and present to the adversary a collectively coherent resilience response. It also shows how each nation needs to develop its own anchor organization and close relations with its IT-relevant private sectors. Its domestic partners agree on a narrative of contribution to systemic defense and then commit to actions in support of that effort nationally and then regionally across industries. Each national anchor organization works to buy time for current defense and to fund the collective transformation of the original inadequate cyberspace into a defensible and democratic digital substrate shared across the CORA nations.[56]

Figure 2. Cyber Operational Resilience Alliance for the Democratic Like-Minded[57]



The CORA is not merely an alliance; it is an operational structure built on the anchor organizations and the cooperation across allied government and private sectors. Two examples of how democracies already have relatively successfully achieved this kind of operational collaboration exist in NATO and the EU. Both are *sui generis* and their survival over time despite both budgetary and economic pressures is promising. There are also other reasons to argue that a CORA is doable. A strategically coherent community of more than 900 million citizens will have the economic market weight and the technological talent pool to face an adversary the size and strategic coherence of China as a peer nearly to scale in a conflictual cybered world. Such a unified systemic cyber resilience alliance can orchestrate its own shared adaptive sensor and mitigation systems, massive R&D programs with universities and firms, and the economic and technological talent to transform the collective cyberspace into what it was meant to be when created nearly thirty years ago. The shoddy substrate can be reformulated to be fundamentally secure, fair, open to global trade, democratic in values, and harder to exploit remotely for economic advantage and cybered conflict, including massive disinformation campaigns.

Furthermore, elements of a future CORA already exist across like-minded democracies in various forms. These include routinized and emergency cooperation across operationally functional industry associations, NCSC equivalents in governments, various operational public-private task forces dedicated to solving specific defensive or offensive problems, and a variety of other (mostly too fragmented) practices in the military, critical infrastructure, intelligence, law enforcement, telecommunications, and IT capital goods sectors of these nations. Gathering these mini-experiments along with the private sector actors responsible for them will enable the collective sensemaking and action commitment needed from both government and IT-relevant private sector. As a collectively integrated and coherent global actor, the CORA can provide the framework and urgency to build the necessary civil consensus needed among its component states. Its structure and mission to maintain a unified all-sector response actively engages the private IT capital goods sector in the defense of the democratic economic system

as team players, citizens, while remaining globally vigorous competitors. Only with such an operational alliance can democratic societies afford the necessarily large push to combine talent and investment. This will keep markets healthy with alternative technologies that are able to transform basic Internet technology at the proper scale and defend the economic wellbeing and democratic values of their nations in the future.[58]

The CORA enables like-minded nations to act in rough unity as a "Great System" in Great Systems Conflict against the authoritarian nations on the rise. Despite being small in number, the community of democratic states acting in unity will be able to present a cybered form of collective statecraft against an adversary's global capacity. The community will be more cyber-autarkic and resilient, risking neither vassal status nor impoverished isolation. In doing so, the consolidated democratic world will create the robust cyber power needed to negotiate from strength with China for equitable international system rules and acceptable societal well-being in the emerging highly conflictual, systems-versus-systems era. The democratic CORA will also enable a successful democratic model of systemic resilience and prosperity for the rest of world's populations to consider going forward.

IV. STRATEGIC COHERENCE AT SCALE FOR RESILIENCE IN GREAT SYSTEMS CONFLICT

Imagine a different world for the moment: one in which we recognize that Great Systems Conflict includes the struggle across socio-technical-economic systems to sustain the regime under which one prefers to live. Imagine our situation today if institutions beyond a cyber command were designed to accommodate a national Great Systems Conflict strategy inclusive of major IT capital goods players, telecommunications and other agencies, and relevant cross-sector/domain organizations. Imagine that all are included in an annual grand strategic huddle to allocate resources, and set forth operational responsibilities and cooperative, enforceable standards for performance. The goal is to iterate and agree on next steps, the R&D and operations funding incentives, the regulations, and the narrative about why this is to be done and how it preserves democratic values.[59] If the world of contesting (and accommodating) multi-sectoral/domain systems were taken as a given, how would it be different now and going forward?

When the democracies show the rest of the world that a democratic CORA can survive under the magnitude of threat sources—even a trifecta—and even innovate beyond the harm, then democracy itself will regain the allure it had fifty years ago, before a shoddy cyberspace, a rising authoritarian behemoth, and a pandemic severely damaged that model. As Ben Franklin famously said, "If we do not hang together, we most assuredly will hang separately." There is no assured future for democracy in the coming decades unless we act to ensure it now and collectively. In late November 2020, the EU floated a plan offering the US in particular new allied ties on technology (cyber), COVID-19 (pandemic) and "democratic interests."[60] The time to move out on collective democratic resilience is clearly now.

Resilience Foremost, Fires Forward, and Allies Always

All the ideas herein are those of the author and do not reflect the position of any element of the U.S. Government.

NOTES

1. Data from the updated GDP cyber erosion analysis given by Melissa Hathaway in 2019 for GlobSec conference. Melissa Hathaway, "Preparing the Future: Assessing Slovakia's Cyber Readiness" (GLOBSEC 2019 (prepared speech), Bratislava, Slovakia, April 29, 2019). See also Abigail Boatwright and Mark A. Wynne, "Record Global GDP Contraction Indicative of COVID-19's Cross-Country Effect," *Dallas Fed Economics*, October 6, 2020, https://www.dallasfed.org/research/economics/2020/1006.aspx.
2. See, for example, the US tendency to learn rarely from previous experiences. R.F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (New York: Macmillan, 1973). David Karlin, "What bugs me the most? World+dog just accepts crap software resilience - Flawless applications are for time-rich people with endless cash," *The Register online* (https://www.theregister.co.uk/2019/03/27/software_resilience/), March 27, 2019. Hal Berghel, "Equifax and the latest round of identity theft roulette," *Computer 50,* no. 12 (2017). 72-76, 113-31.
3. Brian Fagan, *The Little Ice Age: How Climate Made History 1300-1850* (London: Hachette UK, 2019).
4. Uri Friedman, "The New Concept Everyone in Washington Is Talking About: How exactly did *great-power* competition go from being an "arcane term" a few years ago to "approaching a cliché?" *The Atlantic Monthly*, August 6, 2019, https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/.
5. U.S. Cyber Command's 2018 Strategic Vision can be found at https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
6. John J Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton & Company, 2001).
7. Michael J. Mazarr, "This Is Not a Great-Power Competition – Why the Term Doesn't Capture Today's Reality," *Foreign Affairs* (May 29, 2019), https://www.foreignaffairs.com/articles/2019-05-29/not-great-power-competition.
8. General Hermann Balck, *Translations of Tape Conversations with General Hermann Balck*, Battelle Tactical Technology Center (Columbus, OH: Batelle Tactical Technology Center, 1979).; W.H. McNeill, T*he Pursuit of Power: Technology, Armed Force, and Society Since AD 1000* (Chicago: University of Chicago Press, 1982).
9. R. Smith, "The Utility of Force: The Art of War in the Modern World," in *The Utility of Force* (London: Allen Lane, 2005)
10. Three key pieces include one explaining conflict among states as unitary actors, and one placing the states in a system. Kenneth Neal Waltz, *Man, the State, and War: a theoretical analysis* (New York: Columbia University Press, 2001 (1959)). Robert Gilpin, "The theory of hegemonic war," *The Journal of Interdisciplinary History* 18, no. 4 (1988), 591-613. R. Smith, "The Utility of Force: The Art of War in the Modern World," (London: Allen Lane, 2005).
11. Mazarr, "This Is Not a Great-Power Competition: Why the Term Doesn't Capture Today's Reality."
12. T.C. Jespersen, "Analogies at War: Vietnam, the Bush Administration's War in Iraq, and the Search for a Usable Past," *Pacific Historical Review* 74, no. 3 (2005), 411-26.
13. Emily O Goldman and John Arquilla, *Cyber Analogies,* Naval Postgraduate School Press (Monterrey, CA: Naval Postgraduate Press, 2014). George Perkovich and Ariel E Levite, eds., *Understanding Cyber Conflict: Fourteen Analogies* (Washington, D.C.: Georgetown University Press, 2017).
14. Mazarr, "This Is Not a Great-Power Competition – Why the Term Doesn't Capture Today's Reality."
15. Friedman, "The New Concept Everyone in Washington Is Talking About - How exactly did *great-power competition* go from being an "arcane term" a few years ago to "approaching a cliché"?" https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/.
16. P.J. Dombrowski and C.C. Demchak, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs, special issue on cyber* (2014), 29-38.
17. Chris C. Demchak and Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs* Journal 3, no. 1 (October 21 2018), https://scholarcommons.usf.edu/mca/vol3/iss1/7/.
18. Liam Tung, "Microsoft: This is how the sneaky SolarWinds hackers hid their onward attacks for so long – The SolarWinds hackers put in "painstaking planning" to avoid being detected on the networks of hand-picked targets," *ZDNet online,* January 21 2021, https://www.zdnet.com/article/microsoft-this-is-how-the-sneaky-solarwinds-hackers-hid-their-onward-attacks-for-so-long/.
19. Bruno Silveira Cruz and Murillo de Oliveira Dias, "CRASHED BOEING 737-MAX: FATALITIES OR MALPRACTICE? " GSJ 8, no. 1 (2020).

NOTES

20. Emily O. Goldman, "The Cyber Paradigm Shift " in T*en Years In: Implementing New Strategic Approaches to Cyberspace*, ed., Emily Goldman, Jacqueline Schneider, and Michael Warner (Newport, RI: U.S. Naval War College Press, The Newport Papers, 2020).
21. J.L. Casti, *Complexification: Explaining a Paradoxical World Through the Science of Surprise* (New York: Abacus, 1994). Charles Perrow, Normal Accidents: Living with High-Risk Technologies (Princeton, NJ: Princeton University Press, 2011).
22. Re-use of old computational science term to mean very hard and as yet unresolved challenges to national security. Personal observation by Dr. Peter Denning, NPS, October 30, 2020.
23. Louise Comfort, Arjen Boin, and Chris Demchak, eds., *Designing Resilience: Preparing for Extreme Events* (Pittsburgh: University of Pittsburgh Press, 2010).
24. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011).
25. Chris C. Demchak, "Uncivil and Post – Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age," T*he Cyber Defense Review* 1, no. 1 (Spring 2016).
26. Andrei Tchernykh et al., "Towards Understanding Uncertainty in Cloud Computing with risks of Confidentiality, Integrity, and Availability," *Journal of Computational Science* 36 (2019), https://doi.org/10.1016/j.jocs.2016.11.011.
27. Stephen S. Morse et al., "Prediction and prevention of the next pandemic zoonosis," *The Lancet* 380, no. 9857 (December 1, 2012), 1956-65.
28. As reflected the 2018 U.S. Cyber Command's Vision Statement, the need for targeted offense is often debated, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010. For a discussion of the defense-offense debate in cyber, see also Keir Lieber, "The offense-defense balance and cyber warfare," in *Cyber Analogies*, ed. Emily O. Goldman and John Arquilla (Monterey, CA: Naval Postgraduate School Press, 2014).
29. R.L. O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression* (London: Oxford University Press, 1989).
30. J.R. Galbraith, *Organization design* (Reading, MA: Addison-Wesley Publishing Co., 1977).
31. James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory* (London: Transaction Publishers, 2003 (1967)).
32. Erik Hollnagel, David D Woods, and Nancy Leveson, *Resilience engineering: Concepts and precepts* (Farnham, UK: Ashgate Publishing, Ltd., 2006).
33. Mahmood Yousefi-Azar, Mohamed-Ali Kaafar, and Andy Walker, "Unsupervised Learning for security of Enterprise networks by micro-segmentation," *arXiv preprint arXiv*:2003.11231 (2020).
34. L. Sproull and S. Kiesler, *Connections* (Cambridge, MA: MIT Press, 1991).
35. Allyson Chiu, "A pandemic pod could help you get through winter, experts say. Here's how to form one," *The Washington Post*, October 14, 2020, https://www.washingtonpost.com/lifestyle/wellness/pandemic-pod-winter-covid/2020/10/14/214ed65c-0d63-11eb-b1e8-16b59b92b36d_story.html.
36. M. Mastanduno, "Economics and security in statecraft and scholarship," *International Organization* 52, no. 04 (1998), 825-54.
37. Phillip Alvelda, Thomas Ferguson, and John C. Mallery, T*o Save the Economy, Save People First: Targeted Measures and Subsidies for Cost Effective COVID-19 Abatement*, Institute for New Economic Thinking (New York, November 18, 2020), https://www.ineteconomics.org/perspectives/blog/to-save-the-economy-save-people-first.
38. Editor, "The Quickly Spreading Global Cyber Threat - Interview with Melissa Hathaway," *The Cypher Brief*, February 6, 2019, https://www.thecipherbrief.com/column_article/the-quickly-spreading-global-cyber-threat.
39. Gwen Bouvier, "From 'echo chambers' to 'chaos chambers': Discursive coherence and contradiction in the# MeToo Twitter feed," *Critical Discourse Studies* (2020), 1-17.
40. Comment based on a question asked in frustration during personal conversation with Melissa Hathaway, November 2020.
41. E. Durkheim, *The Division of Labor in Society* (Glencoe, IL: Free Press, 1964). Ramesh Chandra, "Adam Smith, Allyn Young, and the division of labor," *Journal of Economic Issues* 38, no. 3 (2004), 787-805. Jonathan Hearn, "How to Read The Wealth of Nations (or Why the Division of Labor Is More Important Than Competition in Adam Smith)," *Sociological Theory* 36, no. 2 (2018), 162-84.

NOTES

42. John C. Mallery, "A Strategy for Cyber Defense (earlier title: Multi-spectrum Evaluation Frameworks and Metrics for Cyber Security and Information Assurance)" (MIT/Harvard Cyber Policy Seminar, Cambridge, MA, Massachusetts Institute of Technology Computer Science & Artificial Intelligence Laboratory Fall (Spring) 2011 (2009)).
43. For a cyber example of this reshuffling, see Eviatar Matania and Eldad Tal-Shir, "Continuous Terrain Remodelling: gaining the upper hand in cyber defence," *Journal of Cyber Policy* 5, no. 2 (June 11, 2020), https://www.tandfonline.com/doi/abs/10.1080/23738871.2020.1778761, 285-301. The concept of graceful decomposition emerges with the early ecosystem literature of the 1960s but was truly adopted by the reliability researchers in engineering or computer systems architecture. See, for example, Charles Shelton and Philip Koopman, "Using Architectural Properties to Model and Measure graceful Degradation," in *Architecting Dependable Systems* (Berlin: Springer, 2003), 267-289.
44. John P. Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Freedom Frontier online (1996)*. See also as exemplar Rheingold's work, H. Rheingold, *Virtual Communities: Homesteading on the Electronic Frontier* (Reading, UK: Addison Wesley, 1993).
45. Chris C. Demchak, "Cybered Conflict, Hybrid War, and Informatization Wars," in Handbook of International Cybersecurity, ed. Eneken Tikk and Mika Kerttunen (New York: Routledge, 2020).
46. Chris C. Demchak, "Cyber Competition to Cybered Conflict," ed. Emily Goldman, Jacqueline Schneider, and Michael Warner, *Ten Years In: Implementing New Strategic Approaches to Cyberspace* (Newport, RI: U.S. Naval War College Press, The Newport Papers, 2020), https://digital-commons.usnwc.edu/usnwc-newport-papers/45/, 47-66.
47. Jennifer W Spencer, Thomas P Murtha, and Stefanie Ann Lenway, "How governments matter to new industry creation," *Academy of Management Review* 30, no. 2 (2005), 321-37.
48. See https://www.ncsc.gov.uk/, Note the struggle to decide on the form and location of the NCSC was not a foregone conclusion. See, for example, the interesting analysis of how things stood before the NCSC was created, Francesca Spidalieri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *United Kingdom Cyber Readiness at a Glance* (Washington, D.C.: Potomac Institute for Policy Studies Press, October 2016), https://www.potomacinstitute.org/images/CRI/CRI_UK_Profile_PIPS1.pdf.
49. See https://www.gov.il/en/departments/israel_national_cyber_directorate. Jasper Frei, *Israel's National Cybersecurity and Cyberdefense Posture,* Center for Security Studies, ETH Zurich (September 7 2020), https://css.ethz.ch/en/services/digital-library/publications/publication.html/e7ad9067-e6f9-422d-a633-5665b9327ba3. For an extended discussion of the rationale and process behind the INCD, Dmitry Adamsky, "The Israeli Odyssey toward Its National Cyber Security Strategy," *The Washington Quarterly* 40, no. 2 (2017), 113-27. See also Lior Tabansky, *Cybersecurity in Israel,* vol. 598 (Berlin: Springer, 2015).
50. For a discussion of how the INCD in particular works with the military, see the following: Lior Tabansky, "Israel Defense Forces and National Cyber Defense," *Connections* 19, no. 1 (2020), https://www.pfp-consortium.org/connections-journals/national-cyber-defence-policies-winter-2020, 45-62.
51. For information on the National Cyber Security Centre (NCSC) of the Netherlands, see https://english.ncsc.nl/about-the-ncsc. For a mid-2010s view of the cyber readiness posture of the Netherlands, see Francesca Spidalieri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *Netherlands Cyber Readiness at a Glance* (Washington, D.C.: Potomac Institute for Policy Studies Press, May 2017), https://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf. See also R.W. Miedema, "Public-private partnerships for cyber security in the Netherlands" (Executive Master Cyber Security The Hague University of Applied Sciences, 2019).
52. Francesca Spidalieri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *France Cyber Readiness at a Glance* (Washington, D.C.: Potomac Institute for Policy Studies Press, September 2016), https://www.potomacinstitute.org/images/CRI/CRI_France_Profile_PIPS.pdf.
53. Notably among these fragmented nations are the US and Japan. Despite increasing concerns about cyber and the adversary, even in the US case going so far as to ban IT state champions from China, a wide variety of actors still operates independently and discordantly in service of the cyber security of the nation. See Francesca Spidalieri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *United States Cyber Readiness at a Glance* (Washinton, D.C.: Potomac Institute for Policy Studies Press, 2016), https://www.potomacinstitute.org/images/CRI/CRI_US_Profile_Web.pdf. See also Francesca Spidalieri, Melissa Hathaway, Chris Demchak, James Kerben, and Jennifer McArdle, *Japan Cyber Readiness at a Glance,* (Washington, D.C.: Potomac Institute for Policy Studies Press, 2016), https://www.potomacinstitute.org/images/CRI/CRI_Japan_Profile_PIPS.pdf.

NOTES

54. Kevin Kohler, *Estonia's National Cybersecurity and Cyberdefense Posture*, Center for Security Studies (CSS) at ETH Zurich (September 7, 2020), https://css.ethz.ch/en/services/digital-library/publications/publication.html/2d-d8caf3-6741-435b-8b4d-a4df92e67bcb.
55. Friedman, "The New Concept Everyone in Washington Is Talking About: How exactly did *great-power competition* go from being an "arcane term" a few years ago to "approaching a cliché"?" https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/.
56. Demchak, "Cyber Competition to Cybered Conflict."
57. Ibid.
58. This material is taken from the author's 2017 public testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Information Controls, Global Media Influence, and Cyber Warfare Strategy, May 4, 2017, https://www.uscc.gov/hearings/chinas-information-controls-global-media-influence-and-cyber-warfare-strategy.
59. The key values of transparency, tolerance, and trust now include privacy – all four need to be ensured in the transformed and secure new cyberspace substrate to be created by the CORA. For a discussion about why to defend transparency in particular, see the following: Jan Kallberg et al., "Defending the Democratic Open Society in the Cyber Age–Open Data as Democratic Enabler and Attack Vector," *The Cyber Defense Review* 2, no. 3 (2017), 129-138.
60. Sam Fleming, Jim Brunsden, and Michael Peel, "EU pitches new post-Trump alliance with US in face of China challenge: Brussels draft plan seeks to rebuild ties with common fronts on tech, Covid-19 and democratic interests," *Financial Times*, November 29, 2020, https://www.ft.com/content/e8e5cf90-7448-459e-8b9f-6f34f03ab77a.