4

GOVERNANCE IN DEFENSE OF THE GLOBAL OPERATING SYSTEM

James O. Ellis, Jr.

> Technology is a useful servant but a dangerous master.
>
> —Christian Lous Lange (Nobel Peace Prize, 1921)

Nearly one hundred years ago, Christian Lange was awarded the Nobel Peace Prize for his lifelong commitment to and advancement of the theory and practice of internationalism, the promotion of greater political or economic cooperation among nations.[1] In his Nobel address, Lange presciently described the essence of the challenges still confronting our world a century later: "Today we stand on a bridge leading from the territorial state to the world community. Politically, we are still governed by the concept of the territorial state; economically and technically, we live under the auspices of worldwide communications and worldwide markets."[2]

Author's note: I would like to acknowledge the significant research contribution to this chapter by Alexander Stephenson while he served as a research intern at the Hoover Institution in the summer of 2017. This chapter builds on the author's 2016 Hoover Institution conceptual essay, "Readiness Writ Large," and draws on a 2016 co-chaired National Academies report and subsequent congressional testimony on US national security space defense and protection.

Lange devoted his life to the pursuit of an unrealized and, increasingly, unrealizable dream—the unity of mankind.[3] His work began before the First World War with the internationally collaborative Inter-parliamentary Union. But, energized by the horrific impact of the conflict, in its aftermath he aligned himself with and represented Norway in the nascent, and ultimately unsuccessful, League of Nations, seeing in it the poet Tennyson's confidence, "In the Parliament of man, the Federation of the world."[4]

Lange's concepts have been updated in recent decades with descriptions of new world orders that have proved in reality to be anything but orderly. It may be more useful for our discussion to advance the concept of the "global operating system," drawing intentionally on computer terminology. This serves to underline the linkage that technology enables in our hyperconnected world and the theme of this book.

An "operating system" is a computer's underlying software framework. It manages the hardware components and enables all other programs and applications. Its responsibilities scale with the complexity of the system: policing activity such that simultaneous users or programs *do not interfere* with one another, ensuring security whereby unauthorized users *do not access the system,* and *establishing formats and standards* that must be met by all applications and users. There are clearly parallels with the myriad banking, market, communication, information, and national security networks that are the hallmark of our globalized world. In a recent *Foreign Affairs* essay, Tim Kaine adds that when travel, information sharing, technology, immigration, and commerce are added, nations are drawn and held together far more closely than ever before. And the post–World War II system of international norms, rules, and institutions—a system the United States played a major role in building—draws countries closer together still.[5]

In a sense, the term "global commons," typically used to describe international resources—including shared natural resources like oceans, the atmosphere, and space—has been expanded to include cyberspace. But this has occurred without the societal norms, governance standards, and security expectations and capabilities resident, for the most part, in the other domains. For my purposes, let us define the global operating system as including not just the neurons, blood vessels, and connective tissue of our global body politic, but also all the data, information, knowledge, and actions that are transmitted on or enabled by them.

This operating system has evolved to include the technologies, customary behaviors, conventions, and, eventually, treaties governing diplomatic, military, and commercial activity. It also includes operational concepts, strategies, nation-states, and attendant diplomacy that enable those norms. Because of its slow, evolutionary character, the system has up to now been able to gradually incorporate technological advances, accommodate stresses, and, to some degree, resolve conflicts in a deliberate manner over time.

In our era, however, the speed of recent advances in global connectivity and technologically enabled capabilities has significantly outpaced the creation of guiding national strategies and policies. The technological advances in—and increased national security reliance on—the global operating system have created a common global "critical infrastructure" that has not been matched by coherent supporting protection and loss-mitigation strategies, clearly articulated policies, and robust defensive capabilities. These gaps have created newfound concern domestically, confusion on the part of allies, and misalignment and misperceptions on the part of potential adversaries. We must now urgently fill policy gaps, find mitigation strategies, and establish new defensive capabilities.

That the global operating system is under siege is unarguable. Even if the perpetrators remain hidden, the evidence is clear, from large-scale cyberattacks to the massive online theft of billions of dollars in intellectual property; from the rampant insertion of trust-sapping "fake news" to the attempted interference in democratic processes around the globe; from shadowy probes of critical infrastructure control systems to highly visible attacks on commercial entities; from unattributable espionage attempts to well-coordinated hybrid warfare inciting cross-border social unrest; from confrontational encounters in the global commons to attempts to fracture decades-old alliances and partnerships. At every level and in every domain, the number and pace of attacks are growing.

Background

Christian Lange, cited above, was part of a centuries-long parade of, first, European and then global advocates for a broader and more effective world order. By reviewing some of those historic efforts, we can gain some insights into the challenges, changes, and lessons of the past that can inform our way forward. To paraphrase Pavlov: "If you want a new idea, read an old book."

Many mark the beginnings of this effort with the Treaty of Westphalia ending the Thirty Years War, a conflict that Henry Kissinger describes as "a conflagration in which political and religious disputes commingled, combatants resorted to 'total war' against population centers, and nearly a quarter of the population of Central Europe died from combat, disease, or starvation."[6] The Westphalian treaty of 1648 enshrined the concepts of a balance of power among signatory states, national sovereignty, and noninterference in another country's internal affairs. As Kissinger further emphasizes, the Treaty of Westphalia was not conceived as a globally applicable system, not because it did not have that potential but, pragmatically and importantly, *"because the then-prevailing technology did not encourage or even permit the operation of a single global system* [emphasis added]."[7]

Despite the significance of the Treaty of Westphalia, a very different group of statesmen assembled at the Congress of Vienna in 1814 to deal with the wreckage of the order created so optimistically a century and a half earlier. Richard Haass succinctly summarized both the imperative and the outcome: "The leaders of the day were so traumatized by what had just taken place that they operationalized the concepts of the Westphalian model, resulting in the Concert of Europe. The concert, as the word suggests, was an orchestration of how international relations in Europe would be conducted" and required the restructuring of a new balance of power from the wreckage of the old, while accounting for both the rise of nationalism and the impacts of the fall of France and the rise of Russia.[8]

Despite the successes and longevity of the Congress of Vienna, its structure and relationships failed in the first half of the twentieth century to prevent two horrific world wars. The causes of World War I and World War II were many and very different. Much scholarly research and countless books have detailed the political, economic, and societal costs and described linkages between the two. Fulsome discussions are beyond the scope of this chapter, but there are certainly lessons to be learned that can and should inform our thinking, especially as we work to strengthen and defend the global operating system and if we are to avoid future large-scale conflict.

Haass sees two main lessons from World War I that may be applicable to our review. First, he notes that world orders, or global operating systems, for that matter, are not automatic or self-sustaining, even when they are patently in the interests of all who benefit from them. The war benefited no one and cost the protagonists far more than they gained. There are real limits to enlightened self-interest and a real balance of power; despite their existence, they were not enough to keep the peace. For our purposes, this argues that creation and sustainment of a global operating system require constant attention and adjustment as situations and circumstances inevitably change. In aviation parlance, there is no autopilot that automatically corrects for what, initially, are small perturbations that, left uncorrected, can spiral out of control. This fact will bear on our subsequent discussion of an appropriate US role in shaping and maintaining the global operating system.

A second lesson is the limits of economic interdependence. Before World War I, trade was flourishing, but the widespread mutual economic benefits did not prevent the conflict. In his 2015 work *Economic Interdependence and War*, Dale C. Copeland finds that the issue is much more complex. The so-called liberal belief that trade and investment inevitably reduce the likelihood of conflict is not always true. He cites as but one example the Japanese fear of loss of resource market access as a proximate driver of Japanese expansionism and aggression.[9] In a sense, Japan's reliance on international trade encouraged rather than discouraged conflict. Here, too, is a lesson that will need to be considered as we attempt, for example, to refine or redefine our relationship with China.

There are lessons, as well, from World War II, one of which bears particularly on today's nationalist, if not isolationist, trends. Haass opines that European and American actions (or lack of them) were responsible for World War II. Here he specifically calls out the unrealistic and unrealized interwar hopes placed in the League of Nations, the failure of political consensus that prevented American participation in this version of "the new world order," the retreat by America into isolationism (weakened and distracted by the Great Depression), and, finally, the policies of appeasement and disarmament that dramatically shifted the balance of power.[10] Here, too, there may be powerful lessons about leadership in actively helping shape outcomes rather than passively accepting what the future brings. The ability to craft a compelling, inclusive narrative will be essential in defining a way forward. As George Shultz often notes, "You have to be onboard at the takeoff if you want to be there at the landing."

In contrast, the post–World War II order, when viewed on a grand scale, achieved many of the objectives of earlier systems. For nearly fifty years, the balance of power, or bipolarity, that marked its essence bounded norms of acceptable behavior, discouraged great power conflict, and brought a multidimensional focus to global stability. A complex set of agreements, relationships, treaties, and supranational bodies sought to address the economic, political, and security challenges confronting a changing world. From the Marshall Plan to the United Nations, initiatives that reflected both realpolitik and traditional stabilizing concepts were created on both sides of the East/West divide. In Haass's view, the United Nations, specifically, reinforced the Westphalian concepts created centuries earlier. State sovereignty, sovereign equality among all states, and nonintervention in domestic affairs were all codified in the UN Charter.[11] To be sure, there were miscalculations on both sides, as conflicts or confrontations in Korea, Cuba, and Vietnam attest; there was also pressure to adapt the United Nations to the realities of a new world order. Stopping or preventing genocide (Bosnia, Kosovo), redressing territorial aggression (Kuwait, Georgia, Ukraine), responding to terrorist attacks (Afghanistan), and preemptively dealing with perceived threats (Iraq, Iran, North Korea) were all tabled for UN action with, as we now know, mixed results.

The current world operating system, which Haass terms World Order 1.0, served relatively well in the second half of the twentieth century, enabling unprecedented collaboration and economic growth while forestalling great power conflict in a bipolar world.[12] If one accepts the computer analogy, I would argue that, in reality, there have been actual and attempted iterations to the operating system, "patches" in computer terminology, that have reflected the creation and dissolution of international organizations, the formation and abandonment of alliances, and the rise and decline of economies, societies, and military capabilities and the nations they support. There has been an evolutionary improvement in the capabilities and capacity of the global operating system. But it is also true that the system has reached its limit; it cannot keep pace with today's challenges and changes. Some, in other contexts, have called for a simple "reset" of the global operating system, but it is increasingly apparent that that will not be enough. The issue is both capacity and speed. A system designed for diplomacy, deterrence, and mutual dependency and defense among nations does not necessarily have the "bandwidth," capability, or resilience to deal effectively with nonstate actors, criminal syndicates, nongovernmental organizations, transnational businesses, or information warfare from whatever source. Similarly, the processes of the past century are not adequate for the present, where challenges come at light speed, in unprecedented volume, and from disparate, diffuse, and, often, dark sources. No amount of automation or artificial intelligence can substitute for erroneous assumptions or ineffective or outdated processes. At the risk of sounding glib, applying more computing power to a flawed process simply gets you the wrong answer faster.

The population of Facebook exceeds the population of the largest nation-state. —Niall Ferguson

Problem Statement

Technology is changing our lives and redefining the structure and elements of the global operating system. Rapid developments in artificial intelligence, autonomy, cyberphysical systems, networking and social media, and information (or disinformation) flow are also profoundly altering the global security landscape. Nation-states have new tools at their disposal for political influence while they simultaneously create new vulnerabilities to attacks. Nonstate groups and individuals are empowered by social media and radical transparency. Artificial intelligence and autonomy raise profound legal and ethical questions about the role of humans in conflict and war.

The role technology plays in the current national security context is an equally revolutionary, if not a wholly radical, departure from the past. Not since the development of nuclear weapons has such great technological change affected so much in the national security realm. From the ability to wage war by pinpointing a human target from thousands of miles away with an unmanned aerial drone, to the ability to disrupt a space program with a computer virus, to the ability to genetically engineer in a kitchen a highly virulent pathogen that could kill tens of thousands—these all represent ways in which technology has fundamentally altered the landscape of the national security space. Additionally, as observed by Raymond DuBois, "High-technology weapons are no longer the exclusive domain of only a few nations." Both smaller states and nonstate actors are adopting advanced technologies into their warfare. This "democratization" of technologies of destruction, alongside those for enhanced communication and surveillance, creates "a threat landscape unlike any we have faced."[13]

From a national security perspective, the concept of redefining the global operating system looms large, prompting questions of resources, authority, and accountability. It can also seem more urgent to put exploration of those concepts aside to focus on a growing list of more specific and more easily defined modernization and recapitalization requirements as we attempt, in a fiscally constrained and increasingly threatening world, to define where to put each invested dollar to leverage to best effect its enhancement of our national security. For example, significant potential resides in weaponry technological advancements, often termed a "third offset" strategy, announced by then secretary of defense Chuck Hagel in November 2014. As summarized by Timothy Walton in the July 2016 *Joint Forces Quarterly*: "Secretary Hagel modeled his approach on the First Offset Strategy of the 1950s, in which President Dwight D. Eisenhower countered the Soviet Union's conventional numerical superiority through the buildup of America's nuclear deterrent, and on the Second Offset Strategy of the 1970s, in which Secretary of Defense Harold Brown shepherded the development of precision-guided munitions, stealth, and intelligence, surveillance, and reconnaissance (ISR) systems to counter the numerical superiority and improving technical capability of Warsaw Pact forces along the Central Front in Europe."[14]

The potentially significant costs, long timelines, technological uncertainties, and rapidly evolving adversaries all complicate our planning for the future, even as we wrestle with the realities of the present. A decade and a half of conflict has left the United States struggling with the cost of recapitalizing air, land, and sea forces ridden hard over many years: achieving the right balance of technologically innovative and classic manpower-intensive capabilities, of conventional and special operations forces, and the potential and limitations of technology across a growing number of domains. Today's decision-makers understand that things are changing. But they cannot yet discern whether they are on a linear track to a wholly new national security environment or at the cusp of a dimly recognizable cycle that returns us to a more technologically advanced version of a world we once knew of peer competitors, increasing confrontation, and, if not a Cold War, at least a Hot Peace.

A Way Forward

But even as one is drawn to these budget details and procurement programmatics that will, inevitably, shape the global operating system and national security readiness for good or ill, there are even more fundamental questions that need to be addressed. It is not my intent to specify all the elements of what could or should come next: World Order 2.0. Instead, I will pose questions and postulate issues that will need to be a part of the effort, not just on the part of the national security enterprise or on the oft-cited "whole of government" approach, but, I hope, applicable to the "whole of nation" and, indeed, global effort that will be required. While details must quickly follow, the fundamentals of military and national security planning still apply, as does George Shultz's aphorism to focus on things that can be done and not merely admire the problem. The first question should be: "What are we trying to accomplish?" followed by the corollaries: "With whom, where, when, and (perhaps most importantly) why?"

Importantly, when we hear the term "security," images of the Department of Defense and the uniformed services and supporting three-letter agencies come to mind. But defense of the global operating system now demands a much broader context and is the responsibility of a much more diverse group. Today's definitions of "national security" and "the global operating system" encompass economic, political, diplomatic, informational, humanitarian, and educational elements. It is no longer just the role of those who wear the "cloth of the nation." If you are reading this, you are or should be a part of the effort.

What?

The national security planning process for operations or contingencies begins with a National Security Strategy. Provided by the nation's senior civilian leadership, it addresses the national interests, goals, and priorities, while integrating all elements of national power and reflecting all extant national security directives. Somewhat confusingly, a National

Defense Strategy, then a National Military Strategy, and, finally, Joint Operations Concepts follow it. This bureaucratic process is often agonizingly slow, and consensus among all involved is difficult to attain. But, when complete, it can provide a context or template against which all national security efforts can be measured and a means of ensuring consistency and coherence in answering the most fundamental of questions: "What are we trying to accomplish?"

The difficulty of this process is well understood by my distinguished former colleague General Jim Mattis. He is famously quoted describing Washington, DC, as a "strategy-free zone." Somewhat ironically, in his current position as secretary of defense, he is now accountable, in part, for that strategy's creation. He is as capable as anyone of that task, but in recent testimony in front of the Senate Armed Services Committee, even he noted: "We entered a strategy-free environment, and we are scrambling to put one together." He continued, "Anyone who thinks an interagency, whole-of-government strategy can be done rapidly is probably someone who hasn't dealt with it." But a strategy for preserving national security and defending the global operating system is essential. We cannot expect that the hundreds of elements contributing to national security can act in concert, absent an overarching concept and consistent, coherent goals. No matter what the national security issue, be it terrorism, cyberthreats, immigration, trade, China, Russia, North Korea, or diplomatic initiatives and alliance commitments, each must be confidently and dependably addressed to avoid confusing friends and enabling foes. We also cannot afford to lurch from crisis to crisis, dealing tactically with what, inevitably, will become problems with strategic dimensions. Tactical energy in a strategic vacuum is a recipe for disaster.

As noted earlier, America's technological revolution has transformed our own national security capabilities, an essential part of deterring and defending against attacks on the global operating system. Our military forces and, indeed, those of allies and adversaries were eager and early adopters and now have capabilities previously unimaginable in every corner and at every level of the battlefield. Terms such as "network-centric warfare" and "information dominance" have entered the lexicon and, in some cases, departed as the realities of both the traditional nature of combat and the growing capabilities of adversaries have closed the digital divide. In the domain of cyberwarfare, the creation of more "information nodes," a euphemism for participants, also creates more potential targets and vulnerabilities; unsurprisingly, robustness and resiliency still matter. This is particularly true at the high end of our military capabilities, such as global communications and sensors, major platforms, and, of course, our nuclear deterrent forces. The newer systems need additional hardening against the cyberthreat; ironically, the age of some elements of the nuclear command-and-control system makes them less vulnerable to today's electronic probes and postulated future attacks. As we recapitalize these forces, robust, flexible, and adaptable cybersecurity elements must be designed in, not bolted on.

It is also true that, driven by the pace of change in the character of the threat, our approach to the development, procurement, and deployment of resilient and adaptive systems must change. It has almost become an article of faith that the government procurement process is an antiquated and bureaucratic process. In the words of defense analyst Loren Thompson, it "is as baroque as it is broke." Study after study has echoed the Packard Commission's conclusion in 1981 that there was "no rational system" governing defense procurement and that it was not fraud and abuse that led to massive over-expenditures, but rather "the truly costly problems are those of overcomplicated organization and rigid procedure."[15] And, finally, we must get it all done faster simply because the threats to the global operating system are advancing faster than our ability to counter them.

To be sure, there is work being done within the Department of Defense. Initiatives such as the Defense Innovation Unit Experimental (DIUx) and the Air Force Rapid Capabilities Office (RCO) are a start but lack the scale and funding to broadly reshape the procurement process. Key elements that must be included, according to former assistant secretary of the Air Force William LaPlante in 2015 Senate testimony, are "strategic agility and adaptability principles" aimed at fielding resilient systems more rapidly—resilient in the sense that they "are inherently resistant to predictive failure." In particular, LaPlante stressed the use of modular designs, open architectures, and "block upgrades" to shorten development cycle times, enable continuing competition, and keep pace with dynamic threats. But what the DoD and the services can do is limited; they are still captive to rigid budgeting cycles, focused congressional oversight, and thousands of sometimes contradictory laws and regulations. An old friend, retired Air Force general Joe Ralston, is fond of saying, "You know when you're in a real crisis because that's when they suspend all the rules!" In many areas of national security, we are there—and it is time to appropriately unleash our world-class developmental, manufacturing, and operational expertise. We cannot and must not wait for the existential crisis to grant us the capabilities we need.

On the practical side, the new capabilities we do have are legion; near real-time imagery, electronic intelligence, drones, nascent directed-energy weapons, and offensive cyberwarfare are but a few. While I often argue that change itself is not hard, the pace and, in this case, the acceleration of change is creating its own set of complications. The resultant challenges include high skill demands on the part of our forces, the lack of precision in cyberattacks, the creation of scarce high-demand, low-density resources, and the need for "exquisite" (near-perfect) intelligence for their effective employment. The speed of our technological advances across specific military programs has introduced or exacerbated the real problem of inadequate communication between our systems, among our services, and, importantly, with our allies. In the case of new technologies or confrontational domains, such as space or cyberspace, our policies and legal or ethical concepts have struggled to keep pace. What does deterrence look like in space and cyberspace, for example, or the concepts of proportionality and discrimination, long a part of the law of armed conflict? Simply extrapolating terrestrial kinetic concepts is patently insufficient.

The military is often accused of preparing for the last war when, in fact, it is the military that is expected to simultaneously "learn from history," deal effectively with today's challenges, and perfectly predict and respond to the future. Ensuring the nation's security and the protection of the global operating system that supports it is a capstone exercise in dealing with risk. In our resource-constrained, threat-rich environment, we simply cannot do it all or expect perfection in every one of those tasks we choose to undertake. Prioritizing the risks that inevitably confront us and deciding, specifically, both what we will and will not do is an essential first step. Nothing of any consequence we do as individuals, as nations, or as a global community is ever risk-free.

Our challenge is to pursue success in each of what I call the Four M's: *measure* risk, *minimize* the risk to the extent possible, *manage* the risk that inevitably remains, and, finally, be prepared with a *mitigation* plan when the next crisis materializes.

Measuring Risk

Measurement of risk is not and has never been easy. The ability to use past or present data to predict future events can be plagued by insufficient data or, as is likely in these days of so-called big data, overwhelmed by far more than we can possibly assimilate. In the national security context, the fog of war has gone digital. Another pitfall is that we analyze the wrong data set or rely excessively on standard metrics or indicators that may not be relevant to our real needs.

Those defining the "what" in defending the global operating system must also understand the wisdom of Pascal's Wager, which reminds us, as we prioritize our many goals and objectives, that the *probability* of an event is not the same as the *consequences* of an event. That is why discussion of nuclear deterrence must still bookend the national security conversation that then flows across multidomain conventional conflict to unconventional warfare and, now, potential confrontations in space and cyberspace.

Modern disruptive technologies can't in general be compared to the wholesale massive destruction of nuclear war. But in some

> *cases, I think there's evidence that nations could be brought to their knees, or societies could be brought to their knees, if attacked by these new technologies.* —Raymond Jeanloz

Minimizing Risk

Measuring risk helps with the next step: minimizing it. The national security domain struggles with discerning the difference between large and small risks and understanding where influence can be most effectively leveraged. At a European strategy seminar some years ago, I sat next to the CEO of a British aerospace firm. During a break, I asked him the key to his corporation's recent success. Somewhat simplistically he replied: "Jim, it's simple. I hire the best people I can get and give them everything they want to succeed. And then I let them do it." Unfortunately, I never got to ask him how he could tell the difference between what they wanted and what they needed, as it seemed to me a question any fiscally constrained CEO would want answered.

And so it is with minimizing risk: the possibilities are limitless, but the resources, whether fiscal or personal attention, are not. So where should we place the focus? Minimizing possible risks in new "operating system" designs is important, but so are reliability and maintainability enhancements to existing elements. Hiring and retaining of quality personnel is one factor, but so is wrestling with the knowledge transfer issues surrounding an aging workforce, declining manpower, and blazingly new technology.

Managing Risk

After assessing the risk with as much definition and fidelity as possible, and then working to reduce it to the lowest levels possible, it is surprising how often organizations assume that what happens next is somehow beyond their control. But risk acceptance is not risk management. This is particularly true with technologies that one may be able to fully employ while only dimly understanding the engineering or electronics that make it all work. A few years ago in Europe I came across an old German military maxim expressing a similar abject surrender of control. It says: "All skill is for naught if an angel wets the flintlock of your musket."

An opposite reaction among those responsible for global security is to strive to constantly and actively manage risk to ever-lower levels. But defending the global operating system does not require one to become a systems engineer, only that one understands fully the capabilities and consequences of one's technology. It requires leading and holding accountable a capable team and cultivating independent sources to confirm assumptions and monitor progress.

As Nobel laureate Daniel Kahneman has observed, effective risk management also requires the courage to trust personal instincts about things that just don't sound right. He describes in his book, *Thinking Fast and Slow*, his creation of a standardized screening process for candidates to join the Israeli military. Using a series of factual questions, on a one-to-five scale that focused on six specific traits, he initially eliminated the intuition of the interviewers as a factor, believing a numerical assessment had more consistent validity. When the interviewers objected to his "turning us into robots," Kahneman reluctantly added a final step. He added the requirement for the interviewer, when all earlier steps had been meticulously completed, to "close your eyes, try to imagine the recruit as a soldier, and assign him a score on a scale of 1 to 5."[16] After several hundred interviews and performance feedback from their commanding officers, the new interview process using the six factors proved to be a dramatic improvement in predicting a soldier's success. The big surprise was that the seventh element, the "close your eyes" exercise, did just as well. From this, Kahneman concluded that "intuition adds value . . . but only after a disciplined collection of objective information and a disciplined scoring of separate traits. . . . A more general lesson . . . was do not simply trust intuitive judgment—your own or that of others—but do not dismiss it, either." Instincts should never be the only rationale for critical decisions, but they can help alert when to ask more questions, decline to accept conventional wisdom, seek a second opinion, or move with caution when “something just doesn’t seem right.”

The very nature of leadership is you better decide before you can know. Those steeped in the humanities are conditioned to be relatively more comfortable and able to handle that. —Charles Hill

Mitigating Risk

Risk mitigation is the fourth and, in some ways, the most challenging of the “Four M’s.” When I lecture in a class on risk analysis here on the Stanford campus, I take great pains to point out that only a small portion of risk mitigation occurs *after* an untoward event. The bulk of the effort involves preparation in both systems design and resiliency and emergency response capability, coupled with thorough training and regular exercises.

Over recent years, roiled by the events in our country and around the world, we have seen our daily focus changed dramatically, driven, in some cases, by perceived attacks on our global operating system from cyberthreats, so-called fake news, continuing terrorist attacks, and political churn at home and abroad. National security professionals have reacted by seeking information, providing assistance, reassuring stakeholders, and beginning to shape a response. Meanwhile our personal reactions, no matter what our political persuasion, have, successively or simultaneously, probably included concern, disappointment, defensiveness, and even anger. But the most thoughtful have certainly paused, stepping back from the press of today’s crises, and considered not just what we are as a nation but what we might and must become after all of this is done.

A principal area in which I believe there are risk mitigation lessons to be learned is in emergency response. It is true that our nation has had a local or regional emergency response obligation and capability for decades requiring emergency plans, emergency response centers, and coordinating or controlling organizations in the case of natural disasters or terrorist attack. Similarly, at the highest levels of the national security apparatus, we have gathered in the "Tank" at the Pentagon or as the National Security Council to address specific international or national security challenges. But how will we respond—and who will—to the large-scale, multidimensional crises that may still confront us?

For example, all of us past our twenties remember the horrific events of September 11, 2001. We remember where we were, how we learned of it, how it changed our lives forever, and some of us still mourn the friends and colleagues we lost. We look back with pride on the way the nation came together, leadership reassurance, and the outpouring of assistance to those affected as our critical transportation infrastructure ground to a halt. We also remember that, despite all of those successes, few would dispute that it was, at best, a pickup game. The chaotic events of those days have clearly shown the benefits of continuing to significantly improve specific plans while moving beyond them to establishing and formalizing a national and international response capability worthy of the name. I wonder, as those events drift aft in our wake, whether we are today as committed and capable as we might someday need to be.

To be clear, I am not talking about merely rewriting plans, creating national or international working groups, and constructing memoranda of agreement. Rather, I am suggesting that we need to consider having, at the ready, a robust, highly capable response team with pre-delegated authority and pre-staged equipment, interoperable both domestically and internationally. This national emergency response organization—which I, tongue in cheek, call NERO, after the Roman emperor who famously fiddled while Rome burned—could be a powerful and, I believe, collaborative effort in which the nation could visibly take a leading role both domestically and internationally, across a broad spectrum of challenges to both our national and global operating systems.

Two decades ago, an element of the Department of Defense coined the term "virtual presence." Then just on the technological cusp of today's ubiquitous capabilities, the concept got a little traction until a clever low-level officer noted "virtual presence means real absence!" That was the end of that concept. In today's technologically networked world, replete with handheld global communication devices, virtual reality, high-definition videoconferencing, and artificial intelligence, virtual presence is now here and must be a key element of a NERO structure that unites the real national "first responders" to disruptions of the global operating system. Regular interactions, comprehensive policy discussions, sharing of best practices, proactive contingency planning, and regular exercises are but a few of the roles for NERO. Technology will allow true national experts who have important "day jobs" to interact regularly and effectively with colleagues around the world without the need to be continuously huddled together in a basement command center behind a sign that reads "Break Glass in Case of Emergency."

With Whom?

An adaptation of a writing of the rabbinic sage Hillel the Elder is often quoted as: "If not me, then who?"[17] For the decades since the end of World War II, when the question was asked in the West, the answer has most often been: "The United States of America." Through the critical days of the Cold War and beyond, in crises of security, economy, or humanity, we were there. On NBC's *Today Show* (February 19, 1998) and repeatedly since, then secretary of state Madeleine Albright famously declared: "We are America; we are the indispensable nation. We stand tall and we see further than other countries into the future, and we see the danger here to all of us." Nearly twenty years later, even if the statement is still true, as I believe it is, there is more than a hint of arrogance and certainly an implied perfection that, in truth, has not been borne out consistently through the incredible range of challenge and change we collectively confronted over the last two decades. Nevertheless, despite the closing of influence gaps and the rise of a new near-peer competitor, America remains the preeminent global power.

Last year, I was privileged to moderate a session of a Hoover Institution seminar on American exceptionalism with George Shultz and the late Sid Drell. In my brief remarks, I opined that *exceptionalism*, which has often been an American hallmark, was not the same as *triumphalism*, which must never be. Returning to Tim Kaine's recent critique of American doctrine and strategy, "Instead of proclaiming its own indispensability, the United States should strive to reestablish its position as the *exemplary* democracy [emphasis added]."[18] No matter where you are in the spectrum of self-defining America's place in the world, one fact remains incontrovertible, if not unarguable: there are things only America can do and leadership roles only America can play.

That is not to say we must or should do it all or go it alone. To achieve and sustain an effective, resilient, and just global operating system across the world, we must establish, by personal commitment and example, not fiat or decree, global standards with international accountability. Believe me when I say that I do not believe it is our job to change the world; I do believe, however, that it is appropriate to support the world's efforts to change itself. Continuing attacks on the global operating system are international events and demand an international response. While the former statement may be self-evident, the latter is not, and I believe that they are inextricably linked.

Let me explain. In the eyes of many, including many of us, historic disruptions of the global operating system laid bare some significant gaps in our performance and effectiveness as a global community. These events, I hope, have swept away reservations of any who thought that events half a world away could not have significant influence on our domestic security, as we now broadly define it. Similarly, to succeed in both countering and containing the threats, any response we craft must have an international dimension. To do less would be, at best, shortsighted and, at worst, sadly ineffective.

My second takeaway from both my own government service and our national crisis response experience over many decades is the value of relationships, both those of long standing, which are often deepened and strengthened, and those that are created afresh with organizations and individuals who share our concern and commitment but with whom we had never before spoken. Each of these stakeholders is involved in different ways for different reasons, bringing specialized and necessary expertise, skills, and resources that, in concert, can provide essential aid to those attacked and information and insight to us all. My point here is to highlight that those who will come together in any crisis of the global operating system may be united by a commitment but not by process, training, or previous interaction. We should not be reduced to creating new relationships on the fly or introducing ourselves for the first time during initial organizational conference calls.

I often speak of silos in organizations, or, as former national intelligence director Admiral Mike McConnell, tongue firmly in cheek, used to call them, "cylinders of excellence." Going forward, we should look at these new relationships with purpose and a strategic objective in mind. The long-term goal should be a process and a structure that cross those industry, government, and private-sector boundaries to enable consultation and collaboration in time of crisis. Our collective efforts in responding to earlier crises have demonstrated what we each can bring to the table. As a nation and as a world, we need to become better at it.

> *Advances in AI will make extraordinarily more complicated coalition issues, not just because of governance, but because of speed at which decisions have to be made, or prior delegation in order to train the algorithms to do it. How do we keep a sense of consultative decision-making in this world?* —Kori Schake

Where?

Throughout our history we have been singularly unsuccessful in predicting where geographic challenges to our national security will arise. Despite modern intelligence technology, we failed to anticipate events in the Balkans, were surprised by the invasion of Kuwait, did not foresee the scope or pace of the Chinese buildup in the South China Sea, and could not conceive of a scenario in which Russia would annex Crimea. The politically and geographically disparate character of the challenges to the global operating system should remind us of several things. First, we need to be better at seeing the world through the eyes of others, be they friend or "other," and not as predisposed to mirror-imaging. Second, our forces, especially land and maritime, need to be regionally present if we are to shape events before they occur, the essence of deterrence. This presence must be balanced by diplomatic representation, humanitarian assistance, and, here, a supportive presence that must be real, not virtual. You cannot surge trust. Third, we need to appreciate that in every case of applying "bleeding edge" technology, we have erroneously assumed that we are thus operating in a secure sanctuary and that, since adversaries do not exist, they never will. We find ourselves then playing catch-up when confronted by inevitably emerging threats, which we are ill equipped to counter or deter. And finally, we need to understand that we will be appropriately sharing the global security burden with others, each of whom brings unique capabilities, insights, and regional security expertise.

We cannot ignore and must not dismiss the international dimensions of our efforts. I believe passionately in the global security community's obligation to work collectively toward a common goal and, in a previous life, spent decades with valued colleagues from around the world contributing, I hope, in meaningful ways to that effort. To sustain and protect the global operating system from challenges around the world, we must help establish and sustain, by personal commitment, not fiat or decree, global standards of behavior with attendant international accountability.

But there are now new and very different "geographies" to consider, one distant and one omnipresent, that have unique vulnerabilities and on whose systems we are increasingly reliant. The first is the space domain, once considered a remote sanctuary and now increasingly accessible, globally essential, and uniquely vulnerable. The second, of course, is the cyberdomain, which, after more than four decades, has literally transformed our world.

As I wrote in the introduction to a 2016 National Academy of Sciences study:

> The national security of the United States is inextricably linked to space and our unimpeded access to the capabilities resident in or traveling through that domain. Since the dawn of the Space Age, all those who have been a part of what was once a race between two superpowers and is now a $315 billion global enterprise, have implicitly understood this linkage. Over, now, six decades, that reliance on space systems has deepened and broadened. What was once only a realm of exploration and national security has grown to include a commercial element that has become so ubiquitous that it has led us to fundamentally redefine the term "national security space."[19]

One overarching conclusion of that study relates directly to the vulnerabilities of the global operating system in that the speed of advances in access and space-borne capabilities has significantly outpaced the creation of guiding national—let alone international—strategies and policies. The technological advances in space systems and increased reliance on them have created a space-enabled "critical infrastructure" that has not been matched by coherent supporting protection and loss-mitigation strategies, clearly articulated and accepted policies, and robust defensive capabilities.

These concerns are even more relevant to the internet and the ubiquitous prefix "cyber" attached to dozens of terms, from "space" and "commerce" to "security" and "warfare." Indeed, when the term "global operating system" is used, many think only of the hyperconnected world in which we live and the incredibly complex linkage of the internet, with all its capabilities, possibilities, and, yes, vulnerabilities. In introducing one of several cybersecurity initiatives in 2013, the Obama administration noted:

> Cyberspace touches nearly every part of our daily lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. We must secure our cyberspace to ensure that we can continue to grow the nation's economy and protect our way of life.[20]

> *It's one thing to deal with Russia, where we have a long history of interactions and joint recognition of the challenges and so forth. How do we put this in the context of a world with nonstate actors and, particularly, someone who is either crazy like a fox or an absolute madman? It strikes me that we've got a whole new set of challenges here.* —Thomas F. Stephenson

When?

In short, we can wait no longer. The efforts at collective solutions to global problems often identify the building of a global consensus on principles, details, and implementation as the most daunting challenge. Regrettably, I believe that the term "global consensus" is increasingly an oxymoron and, even if ultimately achievable, will come at a pace that we all know is too slow to satisfy both our needs and the security expectations of our nations. I also hope that we are not waiting for or proposing the creation of yet another organization, clearinghouse, or global coordinating body. The need is not for more structure or nonproductive bureaucracy; it is for more effective and collaborative use of what we have. This is not the time to engage in long-term discussions on roles and responsibilities or for dramatic shifts in oversight scope or accountability in an Al Haig-like effort to declare "I'm in charge!"

We must expand and enhance the collaborative efforts of which this symposium is a fine example and drive real change in outcomes, not organization, content in the belief that, if organizational changes are necessary down the road, the form should follow function. If we get the "what, when, and why" right, the how will follow. Organizationally, I often note how sidewalks should be placed on a college campus: where the paths are worn in the grass. That is the clear indicator of how interaction really works, in practice, not in theory. We need not and should not try to define that structure first. Again, there is important work to be done now.

For many years, in the much different context of commercial nuclear safety, a few others and I spoke passionately of establishing a "coalition of the willing" and the potential that it represented. I now have come to believe that I, at least, was thinking too narrowly. What is really necessary to deal quickly and effectively with emergent challenges to the global operating system is a coalition of the ready, willing, and able. *Ready* to gird for the battle now, not at some future moving milestone; *willing* to act, not discuss, debate, or delay; and *able* to bring real resources, drive real change, and demand real accountability.

I am not suggesting we abandon those that are not ready for the journey. But we cannot wait for them to prepare fully. We cannot and should not wait to find what some call the "common denominators," which can, if we are not careful and as the mathematicians reading this know, also often include the modifier "lowest." And, finally, we cannot let them slow the pace.

For years, in a previous life, I spoke of the differences between an alliance and a coalition. An alliance has a formal structure, demands unanimity, and often requires extensive debate and concessions to a myriad of partner concerns before acting. The positive aspect in an alliance, of course, is that when it ultimately ceases talking and moves to action, it brings everyone to the task with the strength of numbers and unity of purpose. A coalition, on the other hand, is like the planting of a flag in the ground. A common goal, a shared objective, and full agreement are demonstrated simply by the participation of those who voluntarily rally around the standard. The only metrics are immediate action and real achievement in pursuit of time-critical goals.

Whether we are comfortable discussing it or not, our world, like our societies, is composed of nations and organizations of diverse skills and wide-ranging, variable capabilities. Those that are stronger in expertise or experience, resources or resolve can seize and shape opportunities out of crises that daunt and discourage others. Thomas Carlyle once said, "The block of granite that was an obstacle in the pathway of the weak, became a stepping stone in the pathway of the strong." The image of which I write today is this: those that *can* must *do*, those that are *able* must *achieve*, and they must *lead* so that others may *follow*. They must form or formalize a coalition that is an example and a standard for all.

What keeps gnawing at me is the speed. —George P. Shultz

Why?

When I began this chapter, I thought that this, the final section, would be the longest and most nuanced. I was wrong. What has gone before has convinced me, at least, of a few fundamental truths. First that the global operating system, as I have defined it, is under constant attack and the threat is growing geometrically. Second, I believe that our ability to deal effectively with the diverse and diffuse challenges has declined, even as the importance of doing so has increased dramatically. Finally, I believe that only the United States can collaboratively and collectively lead this effort; only we have the resources, the global role, and the resolve to get it done.

There are some who believe that, weighed down by the burdens of the last decade and a half, the nation has tired of global leadership and that isolationist sentiments are on the rise, fed by populist trends and a growing sense that national priorities lie elsewhere. This is not the first such conversation to take place in the United States. An earlier version occurred in 1947 when President Truman advanced the Marshall Plan and a vision of America's essential leadership role on the cusp of the Cold War. He, too, faced a nation strained by a global conflict and national sacrifice, understandably leery of entangling global alliances, much less a confrontation with the Soviets. Truman was able to paint a realistic, if frightening, picture of the Soviet threat to Europe and warn that if Europe fell America would follow. In a recent *Wall Street Journal* op-ed, Walter Russell Meade noted, "A Trumanist approach—popular but not populist, moral but not moralistic—would start by showing some trust in the American people. To take one obvious instance where popular and elite views diverge: Ordinary people are inclined to favor a firm, decisive response to jihadist threats, while foreign-policy elites tend to worry much more about the possible effects of American overreaction."[21]

Today, we need another such candid conversation with the American people, one that, rather than creating hysteria, both increases understanding and inspires confidence. As Henry Kissinger reminded the US Senate in 2015 testimony with Madeleine Albright and George Shultz, "The problem of peace was historically posed by the accumulation of power, the emergence of a potentially dominant country threatening the security of its neighbors. In our period, peace is often threatened by the disintegration of power, the collapse of authority into non-governed spaces spreading violence beyond their borders and their region."[22] That technology has played a pivotal role in this change is unarguable. On its website, the Center for a New American Security, perhaps reflective of the word "New" in its name, notes:

> Technology is changing our lives. Rapid developments in artificial intelligence, autonomy, cyber-physical systems, networking and social media, and disinformation are profoundly altering the national security landscape. Nation-states have new tools at their disposal for political influence as well as new vulnerabilities to attacks. Non-state groups and individuals are empowered by social media and radical transparency. Artificial intelligence and

automation raise profound questions about the role of humans in conflict and war.[23]

Conclusion

I began with a discussion of the historical context of world order and my corollary for today's world, the global operating system. I have attempted to outline the scope of the challenge to today's system in the context of the failures of those past. There are lessons to be learned. But they are not lessons learned merely because we write them down; something needs to change, to be approached and dealt with differently. These times are very different and in so many ways more fraught with ubiquitous risks and threats, some unfolding at light speed in nonkinetic but equally impactful ways. It is also too easy, and patently incorrect, to demonize the recently emergent and exponentially exploding technologies. Each problem or challenge attributed to today's technologies is mirror-imaged by many more capabilities and benefits that can improve the lives of tens of millions and, in so doing, enhance our global humanity. The growing challenge we face, as Christian Lange cautioned, is finding a way to remain the master of it all and not become its servant, much less its victim. This is a human challenge, not a technological one.

To be sure, the technological and policy debate, followed by real and substantive assessments of the way forward, will demand an unprecedented level of candor and, certainly, confrontation among all participants. Legacy platforms and processes, not to mention policies, must be rigorously examined and questions of current effectiveness and future relevance honestly addressed. The real resource challenge of system replacement must be balanced with the realities of mitigation effectiveness. In the space domain, for example, considering the potential for widespread GPS jamming or an on-orbit electromagnetic pulse attack, we are already hearing calls for a return to a pre-GPS national security world using updated systems of the past such as E-Loran or thumb drive–size inertial navigation systems. Yet, even as we know the questions to ask, we lack even the analytic tools to dispassionately quantify the operational and fiscal costs that must be a part of the answer as we wrestle with the viability of balancing "the way we have always done it" with the costs and uncertainties of technologies yet to be defined. The old naval maxim comes to mind: "Never let go of one rope until you have a firm grip on another." We know instinctively that Abraham Lincoln was right when, in his annual address to Congress in 1826, he said: "The dogmas of the quiet past, are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew, and act anew." But, as we all instinctively know, addressing the difficult realities of defending the global operating system is not, at its heart, a technical issue. It is a leadership challenge.

Organizational management scholar Edgar Schein has written that one of the primary roles of leaders in time of crisis is to absorb fear, not create it, through clear communication, a demonstrated understanding of the problem, and swift, inclusive action to deal with the looming realities. In essence he defines what Jim Collins calls the "Stockdale Paradox" after the storied Vietnam prisoner of war and former Hoover fellow. Admiral Jim Stockdale told him: "This is a very important lesson. You must never confuse faith that you will prevail in the end—which you can never afford to lose—with the discipline to confront the most brutal facts of your current reality, whatever that might be."[24]

And the facts, as I have attempted to describe, are brutal. A recidivist Russia, a forcefully rising China, a capably belligerent North Korea, and a virulent, violent strain of Islam intentionally confront an increasingly fearful and uncertain global community. Robert Kagan, in an article ominously titled "Backing into World War III," writes: "Americans tend to take the fundamental stability of the international order for granted, even while complaining about the burden the United States carries in preserving that stability. History shows that world orders do collapse, however, and when they do it is often unexpected, rapid, and violent."[25] He brings our meditation full circle when he goes on to note:

> For the United States to accept a return to spheres of influence would not calm the international waters. It would merely return the world to the condition it was in at the end of the 19th century, with competing great powers clashing over inevitably intersecting and overlapping spheres. These unsettled, disordered conditions produced the fertile ground for the two destructive world wars of the first half of the 20th century.[26]

I end with a bit more optimistic thought from Secretary Shultz, who, like Admiral Stockdale, has the knack of balancing realism and optimism. In his book *Issues on My Mind*, he reprises remarks he delivered to the Commonwealth Club of California in 1985: "Civilizations decline when they stop believing in themselves; ours has thrived because we have never lost our conviction that our values are worth defending. But America also has a moral responsibility. The lesson of the postwar era is that America must be the leader of the free world; there is no one else to take our place."[27]

It is fitting that I also include a final thought that might have been conveyed by Sid Drell, were he with us here today—and who's to say he's not? I quote from a copy of a book he authored with McGeorge Bundy and Bill Crowe in 1993:

> One of the great lessons of the last few years is that change is sometimes fast and large and good—and also unexpected. What can be said for now is that both hope and danger make this an extraordinarily good time for continued effort. That effort cannot be American alone, but it cannot be much without us.[28]

In a final note, inscribed on the flyleaf of the copy of Sid's book from which I quoted, are the words: "To George Shultz, with warm friendship, Sid Drell."