3

GOVERNANCE AND SECURITY THROUGH STABILITY

Raymond Jeanloz and Christopher Stubbs

I think we've got to have a balance between optimism about what we can do with this technology but also realism about the dark side. —Sam Nunn

Just as advancing technologies are disrupting many sectors of the domestic economy, they are also transforming the international security arena. Diplomacy, deterrence, and direct military action, tools that have long been used to protect our national interests, are being challenged by rapidly evolving technologies that present new problems with no clear solutions. In sum, the power and pace of modern technologies call for developing new approaches to avoiding catastrophic conflict between nations.

In the past, the success of diplomatic attempts to manage such problems as the proliferation of nuclear weapons is in part attributable to the long timescales of years to decades typically involved with developing nuclear technology and weapon delivery systems. In the current era of ubiquitous, near-instant communication, however, today's rapid technological changes have greatly shortened the time for governmental

consideration, decision, and action, even as these changes present complex and difficult new problems.

The governance challenge in this context is to identify and adapt to the interplay between technology and international relations. Equally relevant to the balance between technology and society are internal adjustments within each nation, from cultural and political to economic and technological, but responses should not be so onerous as to preclude technology from making its enormously positive contributions to individuals' and society's well-being.

We refer to this balance as "stability," a condition in which the pace of change—political, technological, and economic—is on a timescale that allows for governmental systems to adapt to those changes while maintaining sufficient equilibrium to allow steady progression toward prosperity. A disruptive technology is one that upsets this stability and induces changes on a timescale that is too rapid for a governance system to keep up. We use "crisis stability" to describe a condition in which sudden, localized events (e.g., regional conflict, natural disasters) do not drive the global system away from equilibrium, and propose here the notion of "technological stability" whereby the international system remains in equilibrium even in the face of high-impact, rapidly evolving—disruptive—technology.

The objective of this chapter is to explore the governance challenges of maintaining stability in the era of post–Cold War international relations and postmillennial disruptive technologies, with the intent of identifying specific objectives for stability. Stagnation, one form of complete stability, is neither beneficial nor desirable, in that change is both the cause and consequence of progress, whether in politics, culture, or technology. However, the goal is to reduce the chances of technologically induced catastrophe for society, including through inadvertent actions or unintended consequences. We illustrate the issues by starting with a brief discussion of nuclear weapons, a twentieth-century disruptive technology having uniquely destructive power.

Nuclear Weapons

Nuclear weapons, the most physically powerful military technology discovered to date, helped end one war and were supposed to change the nature of warfare forever.[1] That was not to be, however, as military conflict has continued relentlessly around the world. Instead, the recognition emerged that boundless, total war must be avoided because of the consequences of using nuclear weapons: the million-fold difference between nuclear and conventional explosives puts nuclear war in a special category of death and destruction.[2]

Warfare thus continues, but with a collective restraint to engage in combat as it was before the development of nuclear weapons. The effect of nuclear technology is to impose restraints, including through deterrence, to prevent attacks that threaten the existence of a state. Strategic alliances extend this deterrence to nations that do not themselves possess nuclear weapons.

During the Cold War, restraints developed in the context of strategic stability between the superpowers, the idea being to establish—among others—conditions for *crisis stability*, by removing incentives to initiate war, and *arms-race stability*, by removing incentives to increase the size or to enhance the capability of nuclear arsenals. The predominant form of Cold War deterrence was through threatened retaliation; for the superpowers, the primary function of nuclear weapons evolved to preventing their use. The overarching goal of strategic stability was thus to avoid nuclear war, the ultimate catastrophe enabled by the then newly discovered technology.

When you put your hand on the Bible, and swear to be president of the United States, that's the least of it. It's when you put your hand on the nuclear button—then you become God.

—Bishop William Swing

New Technologies

In the post–Cold War era the concept of strategic stability has become confusing, all the more so as a much greater number and diversity of actors are involved, from regional and global powers to terrorist and criminal cartels.[3] Is deterrence a reliable strategy under these circumstances? If so, how generally, and how is it to be implemented?

Moreover, the powerful new technologies now emerging give a sense that the pace of discovery is accelerating relentlessly. Technology is mostly viewed as positive—if not essential—for improving health and quality of life, often benefiting society by empowering individuals and increasing economic productivity. Yet many of these new technologies can also be used to inflict great harm. Do new technologies call for restraints and new codes of conduct between nations?

In particular, nonnuclear forms of deterrence show potential for addressing threats associated with modern technologies, notably deterrence through denial and deterrence through entanglement. The former amounts to avoiding or diminishing the effects of an attack, thereby reducing the incentive to attack. The latter—entanglement—is discussed below and may also be emerging as an important force in the nuclear domain.

Table 3.1 lists some of the important technologies that have come into prominence since the end of the twentieth century. The list is far from complete, if for no other reason than that new technologies as well as new applications of existing technologies are discovered every day. Also, it is somewhat artificial in that most technologies evolve in a continuous fashion, intertwined with other developments. For example, the global positioning system (GPS) plays a crucial role in supporting the internet and also in guiding autonomous vehicles, yet it is treated here as a twentieth-century technology and is left out of this listing. Similarly, nuclear technologies and genetically modified organisms are not included.

The majority of these technology developments have a dual-use nature, military and nonmilitary (or, depending on context, harmful and good). Commerce on the internet is accompanied by malware and

TABLE 3.1 Postmillennial Technologies

Information Technologies (IT)	Computers, smartphones
	Internet and Internet of Things (IoT)
	Artificial intelligence (AI)
	Social media
	Digital currency, blockchain technology
Biotechnologies	Genome editing (CRISPR/Cas9)
Space Technologies	Micro- and nanosatellites
	Robotic capabilities
Remotely Operated and Autonomous Systems	Remotely operated vehicles (ROVs)
	Autonomous air, underwater vehicles (AAVs, AUVs)
	Networked autonomous systems
	Robotic weapons

cyberattacks. Self-driving cars are emerging at the same time as robotic standoff weapons. Governments face the difficult challenge of promoting the economic benefits of these developments while protecting their citizens from the adverse impacts of the technology.

Information Technologies: Cybersecurity to Artificial Intelligence

The threats posed by information technologies, driven by enormous advances in computing speed and miniaturization as well as by the growth and pervasiveness of the internet, are recognized by the need to establish such government entities as the US Computer Emergency Readiness Team (US-CERT) and the Department of Defense's Cyber Command to provide defenses against cyberattack.[4] Moreover, the internet of things involves a massive linking of infrastructure that can greatly facilitate daily life but also brings considerable fragility to society and offers a multitude of entry points for damaging cyberattacks. The US government has identified "critical infrastructure" in an attempt to identify particular vulnerabilities to cyberattack.[5]

As is well known, the cyberrealm has already seen massive attacks and even acts of war through hacking, motivating immense efforts for defense of computer systems. In particular, a cyberattack puts critical infrastructure at risk, whether military command, control, communications, and intelligence (C3I) systems; the electrical grid; or banking and other financial structures. Some of these vulnerabilities are arguably of nation-altering proportion. Shutting down access to water, food, energy, and fuel for weeks across a large region could plausibly cause tens of thousands of premature deaths in a modern society, for example. Less dramatic but perhaps more insidious is the use of cyberattacks to undermine governance and stability within a society: the effects may cumulatively amount to an act of war, yet be too gradual to attract necessary public attention.

Potential consequences of cyberattacks include escalation to other domains and even initiation of nuclear war, if the strategic command, control, or communication systems of a nuclear-weapon state were hacked.

The international community is struggling to establish an international code of conduct in cyberspace.[6] The challenges of attribution and proportional response are complicated by instances in which the perpetrators are not part of any national structure. A technical challenge is to provide reliable and rapid attribution methods while preserving desirable aspects of internet connectivity. The balance between security and privacy in this domain is a topic of ongoing debate.

Artificial intelligence (AI), an emerging development in information technologies, shows promise to enhance and greatly speed up decision-making to the point that it is already used as part of many computer applications such as internet searches and identification and categorization of everything from words and phrases to images, video, and sound in electronic files.[7] While there have been breathtaking advances in recent years, AI's successes and—especially—failures are poorly understood. Many AI algorithms involve a large number of nonlinear mathematical transformations and can be prone to unintended or perhaps even unpredictable performance.[8]

Yet artificial intelligence is becoming encoded in numerous computer applications. It is conceivable—if not inevitable—that AI will be incorporated into systems that support critical military and civilian decision-making processes. The potential for accelerating and improving decision-making in complex environments may prove too tempting to resist, and AI could well be used in circumstances for which it is not suited or intended. This raises the possibility of key information being faulty or improperly analyzed, a recipe for disaster and unintended consequences should it ever happen in connection with nuclear or other high-consequence technologies.

A public debate is under way about whether and how governments should actively manage, regulate, and limit artificial intelligence. Some observers are calling for the imposition of restraints while others see this as unnecessarily hobbling an emerging new technology. A case has been made that the ethical, legal, and social implications should be part of the research agenda for artificial intelligence.[9]

Biotechnology

Biotechnology has exploded in capability and applications in recent years, holding great promise for improvements in medicine and agriculture. With its potential for industrial-scale genome editing, CRISPR/Cas9 exemplifies the modern revolution in this arena.[10] However, its power can in principle be turned to harmful use, notably in the development of unprecedented pathogens or other means to incapacitate humans or decimate agriculture.

To be sure, it has long been possible to create effective bioweapons, so it is fortunate that such weapons are not only banned by international agreement but also widely viewed as unacceptable and unjustifiable. Still, monitoring and verification are difficult, due to the small-scale and multiuse nature of biotechnology as well as the rapid pace of technology development.[11] To illustrate the point with an important contribution to medicine, live versions of the virus responsible for the 1918 influenza outbreak were reconstructed in 2005. The pandemic killed

between fifty million and one hundred million people, far more than World War I, and its deadly character is now understood as a result of the research.[12]

> *Risk is no longer isolated—things nation by nation. It's everywhere. Someone gets sick in Nigeria, they're going to be in Chicago in twenty-four hours. It's fact.* —Lucy Shapiro

Space

The trend with space has been a sudden democratization due to commercial availability of rocket launches and the development of small satellites (micro- and nano-sats). Small nations, businesses, and even groups of private citizens are sending hardware into space, a domain that for decades had been accessible to only the largest of developed nations. As with information technologies, most of the expertise and hardware for space technology have shifted away from government control and exclusive access, now residing in the commercial sector.

Space and information technologies are thoroughly intertwined, such that a threat to one is a threat to the other.[13] For an increasing number of national governments, the loss of space infrastructure can mean the loss of intelligence, surveillance, and reconnaissance capability; of communications and control; and of medical, financial, and other infrastructure that depends on internet connectivity. Likewise, these space-based capabilities can be lost through cyberattacks.

Increasing robotic capabilities, such as satellites that can dock and service other satellites (perhaps using robotic grappling arms), can also pose a threat to national or commercial assets in orbit. Establishing shared expectations and rules of conduct, with a clear articulation of consequences for violating these international norms, would likely enhance stability in this domain.

As global society has become increasingly dependent on both space infrastructure and cyberinfrastructure, an attack on either domain can

result in crisis. If nuclear-related space systems or cybersystems are attacked, a nuclear crisis ensues. More generally, all-out attack on space systems and cybersystems and the associated critical infrastructure could result in vast societal trauma, as large portions of the communications and transportation infrastructure are shut down, affecting everything from distribution of water, food, and electricity to provision of adequate medical care.

Remotely Operated and Autonomous Systems

Finally, remotely operated as well as autonomous air, sea, and land vehicles are being widely adopted for warfare and surveillance, in addition to numerous civilian applications.[14] This technology has emerged since the turn of the millennium, and we include it more as an indicator of the accelerating pace of development than because we understand its long-term implications. In particular, low-cost, highly capable autonomous systems can be networked to form powerful yet responsive swarms that could in principle be highly effective in either civilian or military applications. The important point for the present is that there are likely to be major consequences of these developments, but they are not well understood at present.

> *We used to belittle the Chinese and think we always had ten years on them technologically. Now, as you point out, they're right behind us, and oh, by the way, they tell us, "We no longer copy you anymore."* —James O. Ellis, Jr.

Strategic Stability

Here, we retain the Cold War goal of strategic stability, to avoid nuclear war, and broaden it in two ways so as to address the disruptive consequences of newer technology.[15]

First, we acknowledge that certain attacks through other, nonnuclear technologies could trigger a nuclear response. Historically, US policy has left open the possibility of nuclear retaliation to the use of any weapons of mass destruction (WMDs), including chemical or biological weapons. There is also the potential for nuclear response if nuclear forces or nuclear command-and-control systems are attacked by nonnuclear means, whether with conventional arms or by way of new technologies (e.g., cyberattack). The conclusion for maintaining nuclear strategic stability is that it is beneficial, if not essential, (1) to separate nuclear from nonnuclear military infrastructures; and (2) to avoid attack on any nuclear command-and-control systems.

Second, the impact of the new technologies is not limited to their physical power, but includes the overall consequences of their use in aggression. Modern society has developed efficient and effective infrastructures of material objects, human activities, and relationships between all of these. Yet this interconnected web is fragile and therefore presents key vulnerabilities. Thus, we have posited, in examples given above, modes of attack that would bring a country to its knees through massive shutdown of critical and technically fragile infrastructure. Some of these attacks could plausibly cause enormous numbers of deaths, perhaps not as quickly as nuclear attack but nonetheless effective at crushing a society, more likely over days and weeks rather than in minutes to hours.

This amounts to a threat by an external agent to the continued existence of at least a nation's social and political system, albeit not likely to every human life in its population.[16] Consequently, more than one leading scholar of modern technologies and defense identifies cyberattack as the greatest threat to the United States and other nations over the next decade or so, based on expected value of damage.[17] In this regard, the harmful use of biotechnology is another threat with catastrophic potential.

We acknowledge at the outset that far more analysis is needed on the potentially disastrous consequences of technology. Nuclear weapons stand unique in terms of their capacity for causing physical destruction, representing from a technical perspective the preeminent weapon of

mass destruction. Still, realistic assessments of societal impact are needed for all of the modern and emerging technologies, with the primary focus being to diminish the possibility of their catastrophic misuse.[18] In some cases, such as the cyberdomain, the possibility of misuse may be reduced by mitigation of the effects of an attack: resiliency can provide a certain level of deterrence by denial.

Timescales for Instability

With these considerations in mind, we use timescales to distinguish two elements of strategic stability: *crisis stability* and *long-term stability* (table 3.2). The goal of crisis stability is to avoid an existing crisis between two nations from escalating to a catastrophic level. In principle, this form of stability should include a reliable means of de-escalation from the significant crisis. In contrast, a crucial aspect of long-term stability is to maintain governance that reduces the likelihood of potentially catastrophic crises arising in the first place.[19] In sum, long-term stability should provide a solid foundation for efforts to achieve crisis stability.

Short timescales, high stress, inadequate situational awareness, broken channels of communication, and the potential for misunderstanding,

TABLE 3.2 Elements of Strategic Stability

Crisis Stability	Avoid incentive to initiate major conflict from crisis
	Establish and maintain decision-making integrity
	Maintain situational awareness for both sides
	Establish and exercise means of de-escalation
	Slow down pace of response and decision-making
Long-Term Stability	Understand new technologies, advance technological stability
	Establish norms and promote control of technologies
	Enhance resilience
	Avoid incentives to develop new threats
	Promote entanglement

miscalculation, or miscommunication are key challenges for crisis stability. Both internal and external communications are at risk; the first to maintain a reliable chain of command and responsibility within each nation, and the second to provide for clarification and negotiation between the opposing states.

In comparison with crisis stability, long-term stability requires political focus, commitment, and support over extended periods of time, the goal being to establish effective procedures for avoiding major crises. Enhancing confidence between potentially adversarial states is among the features of long-term stability. Ironically, success in eliminating significant crises can lead to a loss of attention by one side or the other, to the detriment of both. Clearly, internal politics plays a role in each nation's level of long-term commitment to actions that enhance strategic stability. The governance structure and protocols that achieve and sustain stability need to be established through joint discussions among all interested parties and cannot be prescribed by a single nation.[20]

Crisis Strategic Stability

Under crisis stability, deterrence is traditionally considered an important means of removing the incentive for a nation to strike first and initiate major conflict. Many regard this to be the primary if not exclusive role of nuclear weapons, for those states that have them.[21] Of course, having a strong conventional military capability can also play an important stabilizing role, in that conventional is far less risky than nuclear response and can, under the right circumstances, provide an effective deterrent.

For the new technologies discussed here, deterrence is compromised by the potential difficulty of rapidly and reliably identifying the perpetrator(s) of an attack. In many instances, this difficulty stems from the technologies being widely available and multiuse, as well as powerful.

Cyber

Rapid and reliable attribution can be difficult for cyberattacks, the result being that deterrence by threat of retaliation may not be credible. One

deterrence option under such circumstances is through denial, removing the incentive to attack by reducing either or both (1) the chance that the attack can succeed and (2) the damage that it can inflict.[22] This requires establishing effective security, increasing resiliency and redundancy of the systems to be protected, and making other demanding efforts.

How much is enough, however? Much more study is needed to answer this question, but we can imagine different levels of fortitude that involve distinct levels of collaboration. Protection from cyberattack by nonstate actors such as criminals and terrorists can be viewed as a common good addressed by international cooperation, for example. Successfully blocking such attacks may therefore be a reasonable objective to be pursued through international bodies, such as the United Nations or Interpol.

On the other hand, the best that one might do in response to attack by a major state is to reduce or slow down loss of capability, for instance in cyber or space domains, a form of deterrence by denial. Alliances may help in quickly replacing communications or satellite infrastructure, but one would expect less opportunity for avoiding complete loss of capability, in comparison with attacks by individuals or small groups.

Deterrence in the cyberdomain is thus expensive and incomplete, but one aspect (denial) has the positive attribute of improving system reliability overall. For instance, resiliency and redundancy make it possible for infrastructure to perform (perhaps at reduced levels) despite natural catastrophes or other malfunctions, whether due to aging components or human error. Of course, the *possibility* that there will be rapid attribution and retaliation can also play a role in deterring external cyberattacks.

On cyber, we should not believe that even if we had an excellent international agreement, that it would deal with the whole problem, or even a majority of the problem. The biggest problems here are not nation-states but groups outside the law.—William J. Perry

---

Space

Commercial and military space-based communications and surveillance capabilities have historically become concentrated in small numbers of expensive, highly capable satellites. The effective functioning of our civil societies and military establishments depends critically on these legacy space assets, which are increasingly vulnerable to new technologies (e.g., cyber) and more conventional threats (e.g., kinetic).

It may be possible to build more resilient space-based capabilities for the most important military and civilian purposes, drawing in part on small satellite technologies. Small satellites can be constructed and deployed far more quickly than large satellites, and reduced capabilities may be at least in part mitigated by larger numbers being rapidly put into orbit. Careful analysis of the costs and trade-offs involved is warranted, as increasing the resilience of space-based systems could make a substantial contribution to crisis stability.

The capabilities of commercial satellites have improved dramatically in recent years, so there is the possibility that these can offer some level of backup for national systems in times of crisis. It is interesting, in this regard, that nongovernmental experts have used commercial satellite imagery to make significant contributions in areas of surveillance traditionally dominated by major nation-states, for example in nuclear nonproliferation and treaty verification.[23]

Command, Control, and Situational Awareness

Establishing and maintaining decision-making integrity generalizes the function of a national command authority for nuclear weapons, so that it applies to all dangerous technologies. Instituting a robust chain of command and avoiding predelegation of the decision to use nuclear weapons to anyone other than the highest authority is the standard for major nuclear-weapon states. Extending that concept to other modern technologies, it would be a matter of stated policy that the highest authority is required for any major attack, whether nuclear, cyber, or

otherwise. Also, reliable and independent channels of communication should be available to the highest command authorities. It is for both nations' sake that these communication channels not be attacked so that they can function properly in times of crisis.

The difficulty comes with dual-use technology, such as space and cyber, as well as with technology that can be used at many levels of severity (e.g., from low-consequence hacking to crippling cyberattack). Out-of-control rogue elements can be highly destabilizing if they successfully launch a major attack, for instance through cyberintrusion. Therefore, it is in the interest of each nation that such actions be treated either (1) as attributable to a national authority; or (2) as a terrorist (or criminal) threat to all.

Similarly, safety and security are essential to ensuring that neither accident nor third-party actions cause a nation to initiate a catastrophic attack. Nuclear-weapon safety, for instance, is intended to prevent accidental detonation of a nuclear weapon due to a nearby explosion (such as for a nuclear weapon located in a region of conventional conflict), the point being to avoid a nonnuclear event inadvertently becoming a trigger for nuclear conflict. Safety and control mechanisms over biological, space, and other technologies can play an analogous role.

It benefits each party in a crisis to ensure situational awareness for *both* nations. This implies avoiding destruction of crucial intelligence, surveillance, and reconnaissance (ISR) systems and their associated communications infrastructure.

The alternative is that either or both nations may be forced to make decisions based on incomplete or unreliable information, with a potential—if not likelihood—of making worst-case assumptions. This is a recipe for escalation and for a crisis spinning out of control. In the case of nuclear weapons, the objective for stability is to avoid either nation being in a use-or-lose position due to unreliable information and to reinforce the proscription against attacking nuclear systems even by nonnuclear means. In the context of space systems under attack, significant degradation of a nation's communications, command, or ISR

capability may trigger major retaliation by that nation, before all functionality is lost.

> *I think if the public understood this system, and how fragile it is, and how things are susceptible to possible human error—I think we'd have demands for changes on this.* —Sam Nunn

Communication, De-escalation, and Pacing

Actions providing general conditions for enhanced crisis stability are important, but actually dealing with a crisis requires communication between (at least) the two states involved. This underscores the need for a hotline between the nations' leaders and a well-understood chain of command on both sides. It is not just a matter of installing emergency channels of communication, but also of exercising them in order to provide assurance that they will function in a time of crisis. Procedures for recognizing and containing crises as well as for de-escalation are worth working out ahead of time, especially if a third party is involved (e.g., two nations responding to a major cyberattack from one into the other, but actually perpetrated by a third nation).

Finally, we note that the essence of crisis stability is to lengthen the time available for observation, decision-making, and negotiation; that is, to slow down the pace of events to the degree possible. As historically developed in the nuclear realm, hotlines and well-established procedures for crisis response can play an important role for pacing as well as informing decision-making and negotiation. This is a realm, however, in which we imagine future integration of AI could be problematic because of its potential to speed up timescales for decisions and because of the added possibility of injecting faulty information or analysis into the crisis-management process.

Many if not all of the restraints proposed above have been considered in the nuclear realm, but less so (or not at all) in the context of the newer

technologies.[24] However, to the degree that these technologies are powerful, multiuse, difficult to attribute, and rapidly becoming ubiquitous, it is essential to examine the destabilizing consequences of their use, especially in offensive actions, lest those technologies all too quickly come back to haunt those who have invented or first deployed them.

I draw a parallel between cyberattacks and the issue of weapons in space—that is, in orbit. In both cases, we've understood these threats, and people have been warning about them for a long time. But every time the issue comes up in Washington, it is dismissed—either legally binding obligations or even the code of conduct—on two grounds. One is that we couldn't verify any sort of limitations. But the other argument, the one that carries the day, is that we, the US government, want a free hand to do this ourselves, and we can win any competition in this area—which I think is mistaken. —William J. Perry

---

Long-Term Strategic Stability

Long-term stability is a generalization of arms control and counterproliferation in the nuclear realm. Its goals are building confidence; reducing the likelihood of crises that could precipitate conflict; and providing a basis for crisis stability between nations. History shows that efforts must be sustained over long periods of time in order to achieve success in arms control. We expect the same in applying the analogy to newly emerging technologies. In some sense, it is the very process of establishing norms, seeking common ground, and otherwise establishing entanglements (see below) that builds confidence between adversarial nations.

Achieving this goal is not easy. It requires as thorough an understanding of emerging technologies as possible. Understanding the consequences of their use is as important as determining what is needed for

their development. A responsible government will want to evaluate the potential threats as well as the benefits from any powerful new technology, so it should ensure that the requisite technical studies are carried out by government, academic, and commercial sectors.

A case in point is Einstein's August 2, 1939, letter calling President Roosevelt's attention to the newly discovered process of nuclear fission.[25] This is not to imply that powerful new technologies ought to be, or necessarily will be, developed for military applications. Quite the contrary—technical study provides the basis for understanding both the need for and means of controlling new technologies, so as to maximize the benefits and minimize (if not remove) the threats posed by these technologies. This balance between benefits and threats and between disruptive impact and society's response lies at the heart of technological stability, to which we return below.

A key question regards potential blowback from military applications of new technologies. There is the utilitarian question of how quickly and effectively others can adopt and even excel with the technology, such that its development and use in a military context is ultimately disadvantageous. Given both the power and ease of acquisition of the newest technologies, this pragmatic issue becomes more important than ever.

In addition, there are ethical concerns about any powerful technology: just because it is available does not mean it should be used. More specifically, how a new technology is to be used, and the underlying norms for its use, need to be thought through for any military application, lest the consequences of use ultimately outweigh the benefits. The ethical and moral implications of new technologies are at least as important as the technical and pragmatic considerations that we have emphasized in the present discussion, especially as military action is as much a projection of a nation's values as a projection of its power.[26]

Objectives

Four objectives stand out for long-term stability in the light of new technologies: (1) establishing a set of norms for use of the technolo-

gies; (2) building resilience into civilian and military infrastructures; (3) reducing incentives for the development of significantly more powerful threats in any given domain (i.e., avoiding vertical proliferation); and (4) providing incentives for controlling the harmful or threatening aspects of the technologies. The last is a modification of the established notion of horizontal proliferation, to account for the fact that many of the powerful new technologies are widely accessible and have multiple uses, including numerous beneficial applications. That is, the assumption has to be that the technology is, or will soon be, widely available to other nations. Biotechnology is clearly in this realm now, and it is plausible that nuclear technologies will become systematically more accessible over time.

One means of developing norms and building confidence that has proved effective is for nations to maintain regular consultations between governmental counterparts, including between military counterparts. These dialogues can be expanded to incorporate tabletop exercises, for example to practice crisis control, and can be supported by unofficial (Track II) meetings in case the two countries are unable to discuss certain topics for political or other reasons.

Agreements on how to handle dangerous military activities, such as incidents at sea and in the air, are also stabilizing, as are advance notifications of military exercises and missile-testing launches. These serve as confidence-building measures and, more explicitly, reduce the chances of an event inadvertently becoming a crisis.

Public statements of policy are also important, whether to explain decision-making processes and topics of concern or sensitivity or to clarify a nation's position on uses of technologies. Adopting a policy of defensive last resort or of no first use is one example from the realm of nuclear weapons. Analogous clarifications need to be made about a nation's chain of command and leadership responsibility for the most powerful of the new technologies. Use policies need to be spelled out, whether for lethal attacks with drones or for the panoply of defensive as well as offensive cyberoperations. Notably, some cyberdefense operations are indistinguishable from, or can be easily misperceived as, acts of offense.

More generally, public rejection of terrorism as having any legitimacy is an important component of long-term stability, because blurring the lines between national and subnational activities is especially dangerous in a world of powerful technologies that can be used by individuals or small groups rather than requiring the commitment of an entire nation.

We point to the unintended consequences of the 9/11 attacks, which were apparently far more successful in destroying their targets in New York and Washington, DC, than the perpetrators expected. Hundreds of thousands have ultimately been killed in Iraq, Afghanistan, and elsewhere because of that single day's attacks. The important conclusion is that many of the new technologies emerging at the start of the present millennium are more powerful than those of past centuries. The unintended consequences, and perhaps even intended consequences, of using these new technologies are poorly understood.

When you listen to the discussions now of major political figures, it's pretty clear that they are talking on a very thin and superficial level about how to handle problems. —Charles Hill

---

Entanglement

Harvard scholar Joseph Nye emphasizes entanglement as offering another form of deterrence based on countries sharing interests in the modern world.[27] Globalization and the large-scale migration of populations from one nation to another—for education, job opportunities, or other reasons—provide one level of entanglement between nations.[28] Economic relations represent another form of entanglement, whether one state views the other as an emerging market for sales, a source of cheap but capable labor (e.g., for manufacturing), or an opportunity for broader investments—from real-estate development to capitalizing the

other nation's debt. All of these investments and relationships offer reasons for maintaining stability and avoiding war.

Entanglement arises from common interests, for instance when (potentially adversarial) governments realize that it is mutually beneficial to prevent money-laundering. Sometimes, there are even shared norms among a wide diversity of cultures, including nations that otherwise have conflicting values: intolerance for child pornography and rejection of chemical and biological weapons are to a large degree in this category. To the surprise of many in the United States, concepts of free speech are more nuanced, with disagreement about appropriate bounds for speech (e.g., "hate speech," political activism, calls to violence) being evident even among allies sharing significant cultural history.

The relationship between the United States and China is an example of entanglement, whereby both countries are economically interdependent to a degree that stabilizes otherwise conflicting—sometimes antagonistic—military, political, and cultural agendas. It would be profoundly painful to individuals, businesses, and the governments of *both* countries were either to initiate war with the other.

Nye acknowledges the false hopes of a century ago, when world trade was thought to make large-scale war impossible, only to be proved wrong by the outbreak of World War I. However, he makes a case for present circumstances being different, with ubiquitous and near-instantaneous communication bolstering an international web of deeply connected economic, cultural, and even political relationships. In any event, while there can be questions about the magnitude of the effect, entanglement with a potential adversary complicates any decision to initiate the use of force and thereby contributes to deterrence.

It is not just that globalization encourages entanglement but that technology facilitates—if not depends upon—the interconnections that lead to entanglement. Global, ubiquitous, near-instantaneous communication both leads to and is a result of entanglement around the world.

It can also be thought of as a confidence-building measure. A case in point is the use of space, which becomes more secure against rogue

actions the more that nations become dependent on—and therefore invest in—the services provided from space. Notably, states that depend on space are averse to the generation of orbital debris from kinetic attack against space infrastructure, even if not their own hardware; aside from loss of services, the debris can threaten current and future satellite orbits. Mutual interest thus becomes the basis for restraint, amounting to both establishment of a norm and deterrence against violating that norm.

To be effective, entanglement should (1) involve as broad a spectrum of the two nations' economic and political interests as possible; (2) engage these sectors as deeply as possible; and (3) respond to potential instability and crisis in as timely a manner as possible. This calls for a partnership between the public and private sectors associated with the new technologies now emerging. More generally, entanglement along with resilience (i.e., deterrence by denial) may in combination provide the best means of avoiding technologically induced catastrophe between nations.

Technological Stability

Our discussion has emphasized the threatening and destabilizing consequences of technology resulting from the potential imbalance between the magnitude and pace of technological change on one hand and the capacity of governance, culture, and politics to accommodate those changes on the other. As the evolution of technology is notoriously hard to predict, governance systems are often playing catch-up after major technological changes are well under way. Technological disruption can be both beneficial and harmful, however, and it is the positive contributions that are—in most cases—the motivation for development of technologies.

It is therefore essential to develop and support technology's benefits while evaluating and learning to control the threatening consequences of its existence and use. This is all the more true because one nation deciding to limit use of a technology does not mean that others will follow suit, especially if there are immediate benefits for adopting that technology.

TABLE 3.3 Technological Stability

Technological Stability	Expand access to positive aspects of emerging technologies
	Protect citizens from adverse impacts of emerging technologies
	Adapt to and exploit rapid technology advances so as to retain stability
	Deter misuse of emerging technologies: denial, entanglement (retribution)

The internet and biotechnology illustrate that what is considered to be the most appropriate and beneficial control of a technology can be a matter of considerable disagreement, even among like-minded nations. The multidimensional balance between the benefits and threats of technology—and between its disruptive character and societal accommodation—is what we refer to as technological stability (table 3.3).

General goals are clear enough, but the most effective means of reaching these goals needs far more analysis and development. Details matter, and it may turn out that each technology will require specialized or even unique approaches to achieving the analogue of arms control, deterrence, and nonproliferation that has served the nuclear realm.

To be sure, not all technologies are threatening, and there is much opportunity for enhancing stability by cooperatively developing and applying such benign technologies. More efficient distribution and use of energy could reduce reliance on vulnerable grids; small satellites could reduce reliance on vulnerable space assets. These are but two examples of the means by which new technologies could be exploited for enhancing stability.

Conclusion

In an international economy in which growth is essential to prosperity, a static system is neither stable nor sustainable. Change is inevitable and

essential. Improvements in technology have played a central role in increasing productivity and improving the quality of life. The governance challenge is to capitalize on the positive aspects of technological progress while guarding against adverse effects, intentional or otherwise. Adverse effects can include not only misuse but also suppression of technology.

There are many examples of information technology being abused, both in the criminal domain and cyberwarfare. Fortunately, we have yet to see an example of widespread abuse of modern biotechnology.

Establishing shared expectations and general principles that can be applied to each of the emerging technologies, in order to deter their misuse or abuse, could lay a foundation for a stable system. Establishing and clearly declaring national policies that conform to these principles could facilitate steps toward a new deterrence regime that would foster stability while allowing for evolving technologies to continue to be a force for positive change.

Specifically, as nations become increasingly reliant on sophisticated systems that are fragile—satellite constellations, electrical grids, computerized financial systems, and more—we need to establish an international security regime that effectively deters attacks on these systems. This regime can include increasing resilience and reducing vulnerabilities, while taking appropriate steps to sustain these systems' societal benefits. Mutual interdependence on these technologies and their associated commons leads to an entanglement that in itself can be stabilizing. In short, some of the challenges of technology—its power, pervasiveness, rapid evolution, ubiquity, and ease of access—can potentially offer a path to new, more resilient infrastructure and to new modes of international cooperation that enhance stability.

What is to be done? We're so far from having answers to that question. Many people in Washington don't even have the question yet.

—Niall Ferguson
