Strategic Security Challenges for 2017 and Beyond

by

Richard L. Garwin
RLG2@us.ibm.com

For presentation to the NAS Membership at the Annual Meeting, May 1, 2017 at 07:30 AM
(Note added post-delivery: In the interest of efficiency, I did not use slides, so none of the Figures was shown or discussed. Cogent questions followed the 30-minute presentation, but I think it inappropriate to respond to them here.)

Thank you for your interest in my views on some of the most important challenges facing the United States. By a "strategic security challenge," I mean a threat that can imperil the United States or the larger world within the next decade or so.

I'll describe the nature of each threat, how we got there, and some of the possible solutions.

None of these is an easy problem; if they were, they would not have persisted so long. Almost all involve constraints of domestic or international law, the interests of other parties, and, of course, problems in reaching agreement on a course of action. From the landscape of existing threats I choose four for detailed attention, as follows:

1. The greatest threat, based on expected value of damage, is cyberattack. Modern society's near-universal dependence on information systems, coupled with the connectivity of these systems via the Internet, makes this threat the top priority now and in the foreseeable future.
2. The second strategic security challenge is North Korea. Throughout its existence it has pursued the development and acquisition of nuclear weapons, and of missiles to deliver them (and other munitions) to distances ranging from South Korea to intercontinental range. North Korea has had a record of non-compliance with U.N. Security Council resolutions and of not fulfilling its commitments under international agreements. It has long had the financial and political support of China, a global superpower, and aside from the direct security threat it can pose, is also a potential disruptor of international security if its force of nuclear weapons were to lead to their acquisition by South Korea and Japan. North Korea might also add nuclear weapons or the means to produce them to the list of items it sells to other states or to non-state actors.
3. The third threat of significance is Iran, which has substantial competence in technology in general, and in the development and acquisition of missile systems in particular. The response to the potential nuclear threat in Iran is much better developed than is the case with North Korea, perhaps because the nuclear threat of Iran was more urgent and the potential for destabilization in the Middle East even greater than that in Northeast Asia. In addition, because its citizenry are better informed and Iran is much more in contact with the world than is North Korea, it was more amenable to a negotiated solution. The Joint Comprehensive Plan of Action (JCPoA) is an international agreement that was implemented in 2016 between Iran and six counterparties to address the Iranian nuclear threat, and I discuss it in some detail in this talk.

4. The existing U.S. nuclear weapon arsenal and its evolution is the fourth strategic security challenge I address here. I rank it so highly because of the great expenditures involved, and one particularly destabilizing aspect in regard to the other nuclear superpower, Russia. This is the potential for accidental or unintended nuclear war on a vast scale because the U.S. silo-based intercontinental missiles (Minuteman) are ready to launch within a minute of being commanded to do so, and such a launch might be provoked by false warning or interpretation.

I will address these threats in order of estimated ease of making progress to reduce the threat: the Iranian nuclear program; North Korea; the U.S. nuclear weapon capability and its evolution; and, finally, most importantly and probably most difficult of solution, the cyber threat to the United States.

Iran and nuclear weapons

In 1974 the Shah of Iran stated that Iran would have nuclear weapons "without a doubt and sooner than one would think." At the time, Iran also stated a need for a large civilian nuclear power program, looking forward to the day when oil would be gone, or reserved for transformation into chemicals. Iran's nuclear ambitions were legitimized by the Eisenhower Atoms for Peace program—a veritable proliferation initiative.

The International Atomic Energy Agency (IAEA) has long stated that a critical mass of U-235 metal is 52 kg, but efficient nuclear weapons could be made with substantially less U-235. If one takes a nominal 20 kg of U-235 per nuclear weapon, the plant that would supply fuel for Iran's sole power reactor at Bushehr could instead provide 32 nuclear weapons per year. That is the rub: the necessity to ensure that not even a tiny fraction of civil enrichment capacity is diverted to the production of highly enriched uranium.

In the few years after 2000, and particularly after 9/11/2001, the United States and most of its allies introduced sanctions against Iran, and maintained that the sanctions would not be lifted until Iran gave up its work that it maintained was strictly peaceful and allowable under the IAEA. The criterion was "not a centrifuge will turn," which was anathema to Iran, for which enrichment had become a "sacred value". That enrichment is not necessary for fueling civil nuclear power is shown by South Korea, for instance, which has a vibrant nuclear power sector, with extensive development and construction of nuclear reactors there and abroad, but has no enrichment capacity of its own.

Javad Zarif, Iran's Foreign Minister, who had been their ambassador to the United Nations in New York, stated in 2014, "If at the time of the imposition of sanctions we had less than a couple of hundred centrifuges, now we have about 20,000. So that's the net outcome."

Although there was no doubt that Iran possessed and was operating gas centrifuges and had accumulated many tons of enriched UF_6—some of it 20% U-235, as documented by IAEA inspections—there was no such international evidence of a nuclear weapon program in Iran, and Iran vehemently denied having such a program.

By giving up the absolutist requirement of no centrifuges operating in Iran, six like-minded powers were able to undertake extensive negotiations with Iran, resulting in the 2015 Agreement,

which entered into force January 16, 2016. These two slides show some of the limitations agreed to by Iran in exchange for immediate relief from sanctions related to its nuclear activities.

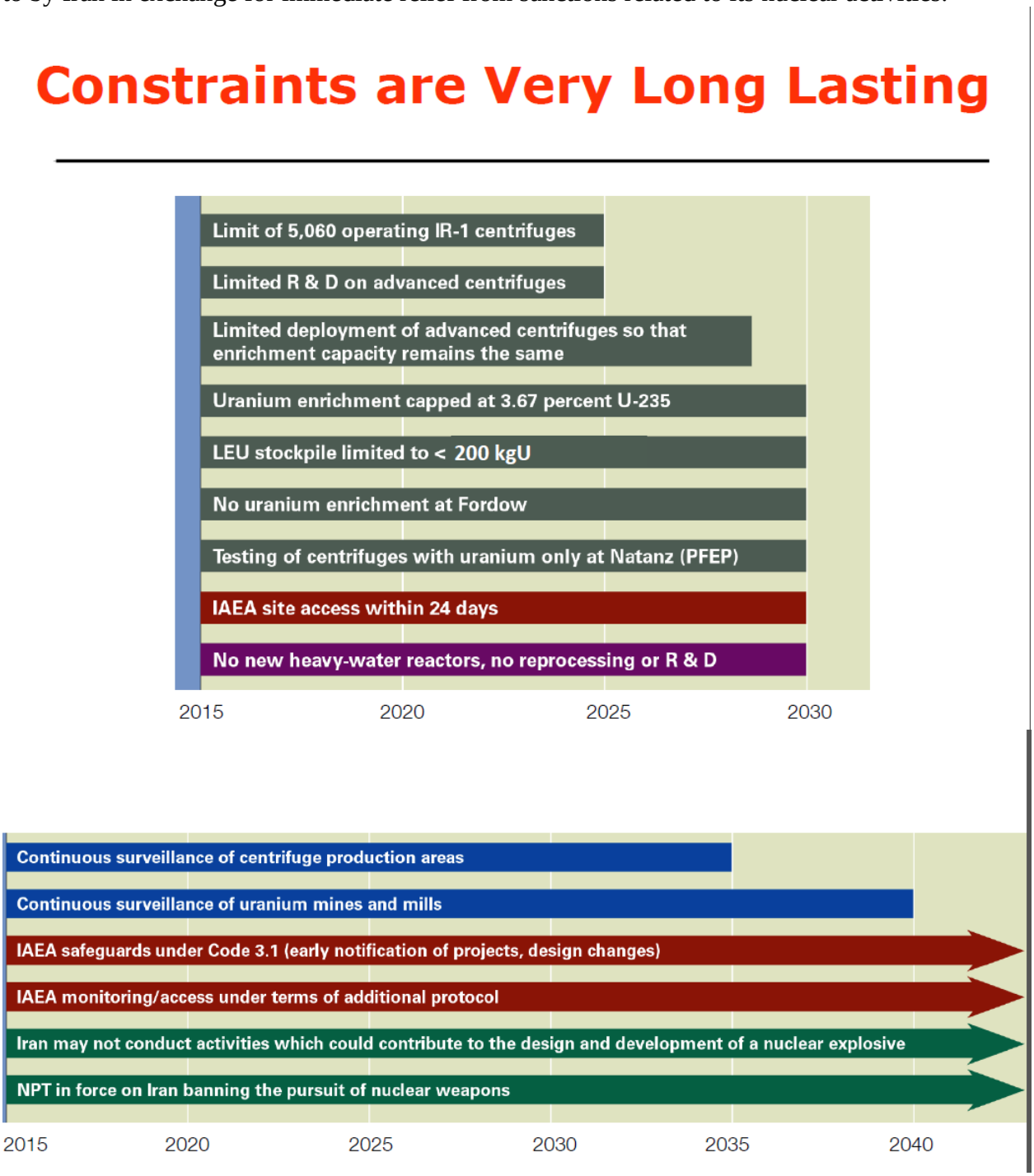

Figure 1. Source: Arms Control Association

In the process of negotiation, Iran shipped out of the country some 98% of its stock of low-enriched uranium, so as to remain below the 200 kg limit of 3.67% uranium set by the Agreement.

The Agreement is 159 pages of mind-boggling detail, with a good deal of room for ambiguity in some aspects, but to my mind it is a great achievement and puts off for a decade or more the time when Iran will have enough enriched uranium for a single nuclear weapon. Moreover, the Agreement denies Iran the acquisition of plutonium for that type of nuclear arm.

If Iran should denounce the Agreement (just as if they had denounced their membership in the Non-Proliferation Treaty and ejected the IAEA inspectors before the Agreement), Iran could, if unimpeded by a diplomatic or military response, use its centrifuge capacity to enrich uranium. But rather than being a few weeks from having enough material for its first nuclear weapon, it would take most of a year—ample time to mount a diplomatic or military response.

So that is the story of one strategic challenge abated, if not solved, as a result of technical and diplomatic effort involving extensive negotiations within the United States, with its allies in the process—including China and Russia—and with the adversary, Iran.

However, some of these constraints expire in 10–15 years; during this time a key objective for the United States should be to use contacts and conversations with Iran to encourage its continued support of the Non-Proliferation Treaty, and to reduce the capacity for nuclear destruction in the world, through Iran's greater integration with the West, and perhaps through reduced security threats in the region. This is a precious opportunity that should not be squandered. For instance, before the end of the Agreement period, Iran might opt for international participation in its expanded centrifuge plant for commercial power-reactor fuel. Yes, a non-nuclear Iran can cause trouble, as it has in Yemen and Bahrain, but a nuclear Iran can do that and far worse.

Since the signing of the Agreement in 2015, Iran and the United States have been on opposite sides of the conflict in Syria, adding to the problems posed by Iran's supply of arms that are used in attacks on Israel. This has led to calls for the reintroduction of sanctions on Iran's missile program, or otherwise pressuring Iran to abandon activities that are contrary to U.S. interests. To my mind, the United States should oppose such activities by Iran, but it would be counterproductive to abandon the protection offered by the Agreement.

North Korea

As a member of the nine-person Commission to Assess the Ballistic Missile Threat to the United States (Rumsfeld Commission), in July 1998 I concurred in the commission's judgment that any of the three emerging powers of that time—Iraq, Iran, and North Korea—

> "would be able to inflict major destruction on the [United States] within about five years of a decision to acquire such a capability (10 years in the case of Iraq)."

We have already discussed Iran. Iraq is no longer in that category, but North Korea definitely is.

In its five underground nuclear explosion tests, North Korea has apparently achieved explosive yields on the order of 10–20 kilotons[1], and may have incorporated, or may soon incorporate, "boosting" technology, in which the exponentially growing neutron population in the exploding

1 (in its test of September 9, 2016)

fissile material is boosted suddenly to a higher level by the rapid fusion of deuterium and tritium within the fissile core.

In February 2017, North Korea tested a solid-fuel missile, which, if the technology is transferred to its medium- and long-range missile program, will make these weapons more robust, easier to conceal, and potentially, with a shorter burn time, more difficult to intercept in flight. North Korea has long sold short- and mid-range ballistic missiles to other states, and has recently offered for sale lithium metal highly enriched in Li-6, indicating that North Korea has no shortage of the source material for producing tritium for boosted fission weapons.

Why is North Korea—with its population of 25 million and per capita GDP of only $1,800[2]—a problem for the United States? The answer lies in the Korean War, which ended, in July 1953, in an armistice rather than a peace settlement, so there is still an armed confrontation between North and South Korea, with the United States allied to South Korea and China to North Korea. The United States based nuclear weapons in South Korea from 1958 to 1990 and still has 28,000 military personnel deployed there.

It is generally felt that the North Korean leader, Kim Jung-Un believes that the United States would take any opportunity to depose him, if necessary by force, and that North Korea must preserve and expand its military capability in order to prevent this.

The United States has been deterred from solving this problem militarily because half of South Korea's 50 million population is in the Seoul area, within range of North Korean guns and short-range rocketry. If North Korea were to initiate a shooting war, making political and economic demands as a condition to bringing it to an end, there would surely be a massive military response, but no one knows how much damage would be done to South Korea before the confrontation ended. Now that North Korea has a stock of perhaps 20 nuclear weapons, the potential damage to South Korea would be much greater, and North Korea could lash out against Japan as well.

North Korea, in turn, has also been deterred from military action—by the threat of massive US retaliation, as well as by sporadic intense negotiations. The United States is concerned (perhaps overly so) about the benchmark that would be constituted by a long-range missile capability to deliver a few nuclear weapons against the mainland USA. This threat is nothing new, in view of the long-standing vulnerability of U.S. coastal cities to attack by North Korean short-range missiles launched from ships near U.S. shores. Deterrence still works, but might be at risk if North Korea's leadership feels that the United States, with some defensive capability, is preparing a preemptive strike.

It has been proposed[3] also by former Defense Secretaries William J. Perry and Ashton B. Carter, that intercept be made "left of launch"—that the United States should destroy the test vehicle for a North Korean ICBM, while it is on its launch pad and not moving at all.

The best approach may be to work with China to provide enhanced sanctions against North Korea, to persuade it not to test missiles to a range beyond 2,000 km and not to conduct further

[2] CIA World Factbook.
[4] "If Necessary, Strike and Destroy," *The Washington Post*, June 22, 2006.

nuclear explosion tests. Success is not assured, and both defense and the promise of deterrence by retaliation against actual use of these weapons are essential. A reduction in the U.S. military presence in South Korea could also be considered, as part of a negotiation to bring North Korea into compliance with U.N. Security Council resolutions.

U.S. nuclear weapons

Our own nuclear weapons can constitute a major threat to the United States—not primarily because of the risk of an accident here or in allied countries, but because they can provoke instability and the use of large numbers of weapons of enormous destructive power.

My involvement with nuclear weapons began in 1950, continuing to the present day. In recent decades this has largely been through work by the JASON group of consultants to the U.S. government in support of the Department of Energy's Stockpile Stewardship Program (SSP).

Since the last U.S. nuclear weapon explosive test, in 1992, each year the directors of the three nuclear weapons laboratories—Los Alamos, Livermore, and Sandia—certify that the existing nuclear weapons stockpile is safe and reliable. By means of extensive experiments and tests without nuclear explosions, and with enormous computational capability, we know far more about our nuclear weapons than in the days of nuclear explosive testing, but there is always the danger of going beyond our certain knowledge and making changes, intentional or not, which will imperil the reliability of the weapons, or cause unexpected problems.

> The very scale of planned expenditures in the Department of Defense and the National Nuclear Security Administration is itself a challenge to our national security, with plans to spend some $340 billion in DOD and $300 billion in NNSA over the next 25 years to modernize and upgrade the nuclear warheads and the their delivery systems—the strategic bombers, the silo-based ICBMs, and the submarine-launched ballistic missiles (SLBMs). Time after time, the U.S. Government has committed to a new weapon or to a modernization program that then becomes unaffordable, resulting in the procurement of a far smaller number of vehicles or weapons—a form of unilateral disarmament.

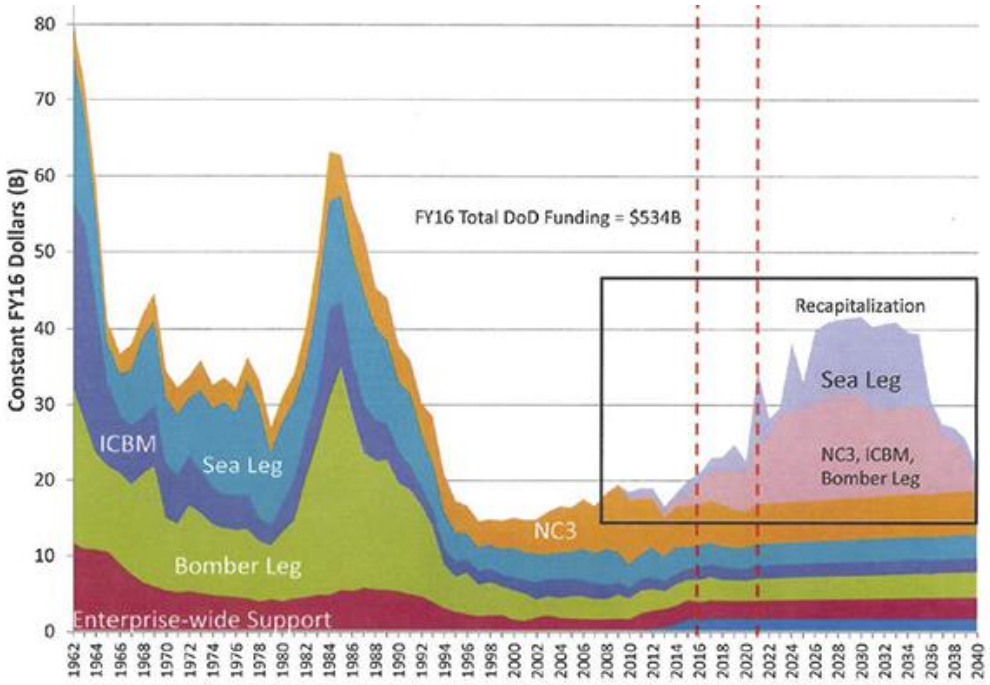

Figure 2. Historical and projected U.S. Department of Defense expenditures on nuclear-weapons delivery vehicles and nuclear command, control and communication (NC3). The two historical peaks are associated with the Kennedy–Johnson and Reagan Administrations. The projected peak is associated with plans for new strategic bombers, ballistic-missile submarines and ICBMs.[4] This does not include expenditures by the National Nuclear Security Administration on nuclear-warhead modernization. (From a forthcoming article by Steve Fetter, Richard Garwin, and Frank von Hippel, to appear in *Physics Today*.)

My own judgment is that a course oriented toward realizing economies can substantially reduce this cost, provide needed improvements sooner, and avoid competitive strategic expenditures in other countries.

My second point it that one must distinguish the role of the U.S. ICBMs (the Minuteman missiles) as regards Russia, from their role as regards nuclear targets in the rest of the world. Russia has enough land-based multiple-warhead missiles (both in silos and as mobile missiles) with sufficient accuracy to destroy all of the 450 Minuteman silos, and this may happen at the outbreak of nuclear war. That very prospect is likely to lead to the launch of all of the Minuteman against their pre-planned targets—most of them, apparently, the offensive (or retaliatory) nuclear weapons in Russia, thus ensuring devastation on both sides, in the vain hope of reducing the damage that would be done to the United States by Russian nuclear weapons.

[4] Department of Defense, Cost Assessment and Program Evaluation, January 2017, https://www.armscontrol.org/files/images/TriadModernizationCosts1.png. The blue band at the bottom that begins in 2012 is funding that DOD has committed to the National Nuclear Security Administration. Most of NNSA's costs for nuclear-warhead modernization, which, by themselves, amount to about $10 billion per year, are in the Department of Energy budget.

According to the late Robert Peurifoy—who died in March 2017, after a long career at Sandia National Laboratories and a second one as consultant to the House Armed Services Committee's Nuclear Weapons Safety Panel—U.S. nuclear weapons today are not significantly different from those that were designed and tested in the 1960s. The two-stage radiation-implosion hydrogen bombs of that era were much safer than even much lower-yield single-stage nuclear weapons, and met many requirements for 100-percent reliability and zero-percent unintended explosion rate, to exaggerate only slightly.

At a time of reduction in numbers of weapon delivery systems, it makes sense to determine the individual margin to failure for each weapon and retain the better ones, rather than replace the entire force—many prematurely. Even better results can be obtained by identifying the best subset of components, and reassembling a smaller number of weapons from them. But few such tools are employed; for instance, such an evaluation exists for the solid-fuel missiles of the U.S. Navy's SLBMs, but not for the solid-fuel elements of the Minuteman.

In short, I favor preserving U.S. nuclear warheads by further life-extension programs, and removing 80% of the Minuteman ICBMs from launch-on-warning status.

Cyber threats

In this ranking of dangerous strategic threats, I put cyber first, and this even without including the potentially effective influence of disinformation and propaganda. The cyber threat is probably also the most obdurate.

The cyber threat is so serious because of the enormous dependence in the United States on computers, and their necessity even to aspects of society that may not present a computer or communication interface to the public. Furthermore, unlike the challenges from nuclear weapons in North Korea, potential weapons in Iran and elsewhere, and our own ready-to-fire nuclear-armed Minuteman, cyber attacks on the United States take place every day, perpetrated by criminals, terrorists, and nation states, with some overlap among them.

There is a strong overlap of the capability for cyber attack with that of cyber espionage, as practiced extensively by Russia, China, the United States, and just about every other country in the world. The United States is not happy to lose information, trade secrets, and valuable data through the intercept of its communications by other states, or from penetration of its computers, whether this is done by remote access from the Internet, or by "close access" by hands-on intervention.

A National Research Council report of 2009[5] provides an early summary of the field. The threat to our society has greatly increased with the ubiquity, now, of the Internet and the increasing penetration of computers into all aspects of modern life.

[5] Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (Washington, D.C.: National Academy of Sciences Press, 2009)

This is about to escalate further with the rapid expansion of the Internet of Things (IoT)—the proliferation of Internet-connected speakers, voice-actuated personal assistants, thermostats, controls of lighting, and the like. There is every indication that the Internet will soon have 100 billion individually addressed gadgets worldwide, augmenting the threat in two ways: First, there are that many more nodes that can be co-opted in a "botnet"; and, second, the protection of IoT gadgets is far less effective than that of even a residential PC, which can have anti-virus suites, automatic software upgrades, and the like. Some cyber threats are very simple, such as a distributed denial of service (DDoS) attack—in which as many as a million individual IP addresses are commanded to send brief signals to a target address, flooding it with so many incoming messages that it cannot handle real ones, or maybe any at all. Criminal botnets are organized as a business, by cyber criminals who have no interest in the specific targets of their crime, but simply rent the tools to perpetrators.

Beyond this simple exfiltration of data, and the installation of tools that use the targeted computer system or computer system network to do the selection of data to be exported, there are the further threats of "preparation of the battlefield," which could be practiced by nation states, in preparation for a possible cyberwar or cyber component of kinetic conflict.

Actual damage to the computer system itself was practiced against Saudi Arabia by Iran in 2016, and against Sony Pictures in 2014 by North Korea. In a different category is the computer-directed transfer of funds, as apparently was practiced by North Korea, and, beyond that, to cyber-augmented sabotage, such as shutting off power transmission lines, with the causing of a massive flood by opening sluice gates from a major dam, or the over-pressuring of a gas pipeline, as practiced by elements of the United States against the Soviet Union, apparently in retribution for their theft of industrial control software.
The picture is indeed grim, because of the many current practitioners of cyber skirmishes, and the fact that economic collapse can be produced by targeting less sophisticated and less well protected computer systems.

As with any threat, the first means of nullification is thought to be "defense," invoking the image of walls and shields, and, of course, there is a lot of defense against cyber penetration and cyber attack. In the case of nuclear weapons, the destructiveness of a single nuclear weapon so far exceeds that of a high-explosive bomb of the same weight that after the early 1950s primary reliance has been placed on deterrence rather than defense. This is not because deterrence is preferable or more moral, but because defense at the required level of effectiveness has been considered infeasible. Deterrence, and its more sinister sibling, compellence, involved manipulating the views and actions of decision makers by the promise of imposing unacceptable costs.
Two recent papers attempt to provide solutions to the cyber threat in this mold, one by Joseph S. Nye[6], who asserts that *deterrence* in cyberspace can be achieved, at least in part, by *threat of punishment*, by *defense* (preventing significant gain from the act), by *entanglement*, and by *norms*. But to what extent and against whom?

[6] "Deterrence and Dissuasion in Cyberspace**,"** Joseph S. Nye Jr., *International Security* Winter 2016/17, Vol. 41, No. 3: 44–71.

A current discussion from the point of view of the U.S. Department of Defense is afforded by its Defense Science Board.[7] This report provides useful information, such as,

> "The United States views cyber espionage as a legitimate activity, and undertakes it extensively; yet, just as with espionage conducted by human spies, there should be both limits and consequences to being caught."

The report cites as examples of significant cyber operations: the 2015 theft by China of 18 million personnel records from the White House Office of Personnel Management, which included security investigations; the 2016 Russian hack of the Democratic National Committee and emails of various public figures, and the disclosure of such material on Wikileaks, with the intent of influencing the 2016 Presidential election; and the 2014 cyber attack by North Korea on Sony Pictures, either for compellence or in retaliation for a Sony film about the North Korean leader.

All of the deterrence solutions discussed depend on reliable, and probably publicly credible, identification of the perpetrator ("attribution"), possibly on a short timescale—with no apparent path to this goal.

What to do, then, until the (cyber) vaccine arrives?

The greatest threat to U.S. security would not seem to arise from an attack directed by the Russian government or the Chinese leadership, as such attacks can, in principle, be deterred by threat of retaliation, whether in the cyber or another domain, even given the imperfection of attribution. Rather, the danger could be greatest from a nihilist or terrorist group that would derive no direct benefit from the devastation it sowed in U.S. society. But even Russia or China could not be expected to abstain from cyber warfare in the presence of armed conflict.

Many potential crimes in U.S. society are prevented not so much by hardening the target, but by near-elimination of the benefit to the perpetrator. Thus, almost any one of us could be murdered outright, and there are many ways of doing that which would hardly expose the perpetrator to certain capture and punishment. But for the most part, the motive could be to obtain ransom from not carrying out the threat, and this requires the ability to transfer money or other material of universal value to the perpetrator. Thus, it is believed that a significant reduction in drug trafficking (or at least an increase in the price of drugs) was effected by the elimination of all U.S. currency denominations above the $100 bill. You can't put $1 million in hundred dollar bills in your pocket, unlike the few minutes it took me to carry three $10,000 bills a hundred meters from the bank to a law office in downtown Manhattan in 1955. Well, it wasn't $1million, but it could have been.

Against the cyber threat of societal destruction, improved likelihood of attribution would help to deter the most able perpetrators. Against the others, various forms of defense are probably the

[7] *"Report of the Defense Science Board Task Force on Cyber Deterrence,"* co-chaired by Dr. James N. Miller and Mr. James R. Gosler (February, 2017) casts the challenge and the solution as deterrence: "*Deterrence by denial* operates by reducing the expected benefits of attack, while *deterrence by cost imposition* operates by increasing the expected costs."

best approach. Yes, norms and agreements can help. But not against the cyber nihilist or cyber terrorist.

Knowledgeable government and non-government organizations know pretty well the path to take to a more robust Internet-like system. But there are major and sophisticated forces on the other side—including some of the same organizations—that see profit in maintaining "transparent" systems, which are incidentally hard to secure against cyberattack.

Many of the threats involving the public Internet are exacerbated by the business model of "cost-free" access and advertising support. A fee-for-service Internet could be offered that is free from the near-universal commercial intercept of the interaction with websites; it would also be much more responsive, while still allowing distributed caching and access to large files.

An added complication with cyber security is that most of the infrastructure and capability are in the private sector, not the domain of government, and yet government is held responsible for and has an interest in protecting the nation from existential threats. Space and cyber share this characteristic.

Much more needs to be done, and quickly. The Department of Homeland Security has much of the responsibility for creating and coordinating solutions to the cyber threat to society, government and critical infrastructure. The current status may be viewed at its site.[8] Beyond bringing existing systems up to current best practices, real research must be expanded in harnessing artificial intelligence to discover and fix vulnerabilities, in creating provably secure programming systems, and in automatic logging and alarming of threats internal to the networks.

Closing Remarks

I have tried to give some background as well as some specifics on these strategic challenges for the immediate future—to some of which we have no early solutions, but for which rational individuals and governments together could lessen their likelihood or potential consequences.

For most of these challenges, the work of our intelligence community is key, as is its interaction with the Congress and the Executive and, ultimately, with the commercial world.

Comparing the vulnerability of our finely tuned industrial and commercial society with that of a century ago, we see that technology has brought enormous benefits and also a great fragility against concerted attack, or even natural events such as a geomagnetic storm induced by solar activity. To inflict starvation and disruption, the cyber threat need not actually destroy much of value, except connectivity. And much of the malign impact can come from a simple loss of confidence— bank failures, lack of trust. A single firm may undergo bankruptcy or even use it as a tool, but bankruptcy is not an option for the United States.

Most of the problems we face need mutual esteem, confidence, and collaboration; without those features the society we have built will collapse.

[8] https://www.dhs.gov/topic/cybersecurity