**The Effects of Nuclear Weapons on Political and Military Strategy:**

**Lessons for the Very Different Realm of Cyber Strategy**

**DARPA National Security Seminar Talk**

**Robert Axelrod**

**October 21, 2015**

Abstract: It took the fifteen years from 1945 to 1960 to work out the major strategic implications of nuclear weapons. For example, before nuclear weapons military strategists valued flexibility, whereas afterwards they valued the very opposite, namely credible commitment. It has now been eight years since the first cyber attack (on Estonia in 2007), and everyone is still trying to figure out the major strategic implications of cyber technology. Despite the great differences in technology and political context between nuclear weapons in the Cold War and cyber technology today, there are valuable lessons that may well apply. This talk will present eleven of these lessons.

The topic I'll be talking about is the effects of nuclear weapons on political and military strategy, and what we can learn about lessons for the very different realm of cyber security. I met with the Director a few months ago, and we batted around a whole bunch of ideas. And this is the one she suggested would be interesting to develop.

First I want to establish that we all understand that there are huge differences between nuclear weapons and cyber weapons, or various forms of cyber technology.

And just to establish some of these important differences, but just a few of them, the problem of attribution, of course, is a very large one in cyber. Whereas if you saw a missile coming from the Soviet Union, you knew who hold to hold responsible for that. But now we have non-state actors, terrorists, activists that could also be using cyber weapons.

Another major difference is that, beside the actors, is that there's no gap in the escalation ladder. In nuclear affairs, everybody understood that the first use of a nuclear weapon in a conflict was a very big deal, a very big jump. If we used it in Korea, or Vietnam or elsewhere, that would have been huge. Whereas cyber, of course, there's this continuity from small to large. And there's no obvious place where there's a big gap. And that makes this strategy more complex.

Another one is that it's very much information-based rather than physically based. An atomic weapon is a physical thing. But cyber weapons are largely about a matter of information, such as zero day exploits. And some of those capabilities can be cheap. To develop a nuclear weapon is not beyond the capacity of poor countries like North Korea and Pakistan, but it's not something you do in your backyard.

Another difference is that the technology of nuclear weapons did change over decades, but relatively slowly. So you had a big transition from atomic bombs to hydrogen bombs, for example, and several other transitions. But for the most part, what you need to know was that one missile can kill one city. You didn't have to know all the details of how that works. And there wasn't much to do to defend yourself.

And so it was relatively straightforward. Whereas, of course, there is very fast evolution in the cyber world. For example, reputation management from eBay, or Uber, or Airbnb is now well established. And you can get voluntary peer recognition for things like contributions to Wikipedia and Linux that allow for very large-scale construction of software. Social media in last few years, that has taken the world by storm. And even the world of zero day exploits, there's obviously a kind of an arms race. And there's even a market for them. So the technology of cyber changes much faster than the technology of nuclear has.

In the political context, the nuclear era of the Cold War, of course, was mainly a bipolar conflict. Not completely, but largely. There was only one major rival for the United States. And there were pretty tight alliances like NATO or the Warsaw Pact. Although there's a lot of competition in the third world, there wasn't the kind of complexity that there is now about multiple great powers.

And the other thing, the Cold War, there was a universal ideology of communism that was our rival that purported to be relevant to all parts of the world. Nowadays, Russia doesn't have a universal ideology. And China doesn't really purport to have one either, other than the combination of markets and authoritarianism.

Where we are today in the political context, in a very brief form, is that Russia has a self-image of deserving respect as a great power that they're used to from the Cold War. They feel that they deserve an equal status to the United States, and they don't get it. And especially that they're deprived of the near abroad, that NATO expansion is just something that they're still resentful about. And you see this on their periphery.

So they're an unsatisfied power looking for respect as much as anything else. And you see this in Syria, for example, as well Ukraine.

And China. China's long-term view of itself is the Middle Kingdom. They were in fact the center of an international system with tributaries on the borders that were mostly less advanced civilizations. And so they feel that restoring that status as the major power, around which other things happen, is sort of the natural thing.

They don't expect it to happen again, but they do expect at least to be able to stand on their own two feet and be respected as a nation, as opposed to the 19th century, for example, when there were the Opium Wars where Britain told the Chinese government to allow imports of opium, because they wanted to sell their product to trade for tea. And China said no, we don't want opium. And Britain said, take it or else. And then they said, or else. And then they had a war, two of them, to import opium. So that's the Chinese idea of what the rest the world does to China when they're weak, and what they'd rather not go back to, and what they'd like to assert is just inappropriate.

Now it’s interesting that China hasn't fought even a small a war since 1979. That was 36 years ago when they attacked Vietnam for a month. The last big war they had was in Korea, 62 years ago. So nobody in the Chinese army has any major military experience. That’s very different from the United States or Russia.

So now I go to some of the lessons. And what I want to emphasize about these lessons is that most of them provide sort of existence proofs. These are things that are possible, things you should be aware of, things that are surprising, and that might be relevant again in a different way, but not necessarily that you would be expecting exact duplication. That's why I gave the differences first.

The first lesson is that is that doctrine lags technology. Which isn't surprising. But what is surprising is the length of the lag. In the nuclear world, it was 15 years from '45 to '60 before even the basics of how nuclear technology would affect political and military strategy was understood.

And that was, for example, from Thomas Schelling who won a Nobel Prize for this work and others. And he established that the standard military view that you want to have as much flexibility as possible is no longer the basis of military strategy. As you know, military strategy has its conventional wisdom that, as soon as the battle starts, the other side is going to do surprising things. And you're not going to know how it's going to come out. So you really want to maintain flexibility in your operations.

This is a very deeply entrenched, very sensible idea. But in the nuclear world, it's completely different. For example, the United States wanted to protect West Berlin when it was surrounded. And we had a garrison there whose purpose was to die, to demonstrate that we would fight a war when that many people died.

We didn't want the flexibility of being able to evacuate it. We did not want that flexibility. And so there's a whole bunch of analogies about people that are tying themselves to railway track and throwing away the key. So the second lesion is that the very basis of military strategy can change with new technology. Before the nuclear ear flexibility is a good thing, and then flexibility became a bad thing. And this took quite a while to absorb, both intellectually, and especially institutionally.

Now that we've understood that, it looks like a relatively easy problem. But at the time, it wasn't. And so all these things about cyber strategy and doctrine, and effects of its technology that look very complicated, are similar to the way that, for 15 years, they looked very complicated for nuclear too.

So it's sort of like when Einstein said space is curved. That assertion wasn’t obvious, but once it was understood, it did make good sense. Perhaps cyber strategy will be like that.

In terms of the timing, you might say if we start with Estonia as the first cyber attack, then that's 2007. So we're halfway there. So it's not surprising we haven't figured it all out. Or if you take Stuxnet as the first major industrial operation by nation states, then that's only five years. So we have some more time.

So let me just list some of the doctrinal questions today that we're puzzling over. And I'm sure you can provide many more examples. But one is how you hold people responsible. If somebody attacks, then is it the governments doing it, or somebody else doing it? And even if it's something in between, then how you hold them responsible?

Another question is active defense. Under what conditions is it appropriate to reach out and interfere with the attack that's coming at you?

Another question, of course, is delegation of authority. In the nuclear world, we had a very simple answer, which is only the national leader can provide the authority to use a nuclear weapon. And this is still an open question, and partially resolved today. But there's a pushback from those who want to have more delegation on the basis that you need to respond in computer time and not in human time.

So delegation presumably takes you at least a few hours to achieve. And then for some purposes, that's not the timescale that you want to react at.

Another doctrinal question that's being kicked around of course is the integration with kinetic warfare. And the trend now, of course, in the United States, especially, is to move it to the regional commands so that they'll have their own cyber capabilities and they'll integrate it with their war fighting capabilities, as opposed to the earlier notion that it would be like nuclear and be completely separate.

And likewise, CyberCom is an institutional embodiment of the separation idea. But the movement to the regional commands would be the idea that you want to integrate it with kinetic. But then the questions arise about, again, more about authority, and doctrine, and usage if it's going to be moved to that level.

Another doctrinal question is what are the incentives for cyber security? Cyber security is obviously really hard, and it's obvious too that in the United States especially, much of what we need to protect is critical infrastructures in private hands. And who's responsible for that? And this is an ongoing issue, of course, both legal, and institutional, and budgetary.

The Israelis take a quite different view. And the government takes much more responsibility for cyber security in industry than we do here. And so that's an open question that still needs to be resolved. And we're working on it.

Another doctrinal question is how much can we develop international norms on the use of cyber? And of course, we had a recent agreement with China that makes some progress in that direction. China and Russia have got another statement of their own. And Russia and the United States have got another statement. So we've got these three bilateral statements all about cyber norms. So that's gaining a little power and steam.

But to what extent, what kind of norms do we want? And what kind of norms can we rely on?

And there's the question of self-restraint. What things shouldn't we do? And the example of nuclear weapons, of course, is that we don't use nuclear weapons, even though they would make the Korean War, for example, a lot easier. But we don't use them.

So what are the self-restraints in the cyber world that we might want to with? The ones that we've done already are financial. We could have taken all the money out of Milosevic's bank account. And we decided not to. And the reason, of course, is that the Treasury Department says, if we did that, then other people would monkey with the financial system.

And we don't know how unstable that is. We don't know how secure-- how stable the world financial system is. Not so much in terms of technology, but in terms of trust. If people weren't confident in it, then the world economy would be in bad shape. So we're going to restrain ourselves, even though we have a lead in this. And even though in a particular case, it might be helpful. And so what other restraints do we want to have?

And a final difference is the relationship between war and peace. International law and behavior has tended to make pretty sharp distinctions. So the day before Pearl Harbor, we were at peace with Japan. The day after, we weren't. And we also declared war on Germany while we were at it. So most large wars especially had a very clear beginning and a very clear distinction between peace time and wartime. And we operate on very different circumstances. You can kill an enemy soldier in wartime. But you can't kill an enemy soldier in peacetime, and all sorts of rules like that.

The cyber world it clearly tends to blur the distinction between war and peace. The nuclear world did not blur that. If you use nuclear weapon, that's obviously war. But the cyber world can blur it in a way that makes it very hard to understand whether an action is a peaceful thing or not.

Now most cyber activities have been on the peaceful side. But I think you could argue that Stuxnet could have been regarded by Iran as an act of war, and some others. But you can certainly imagine lots of cyber activities that would be at large enough scale that they would count as an act of war. And the fact that there's not a clear division calls into question all sorts of things about the nature of the assumptions we make about what is appropriate behavior.

As I’ve said, doctrine lags the technology by years. And then it could reverse some of the fundamentals. The idea of commitment is more important than flexibility.

And let me give you an example of this in from the Cold War. McNamara asked McNaughton, his aide, to write a one-page memo on why we're fighting in Vietnam. This was in the middle of consideration of escalation. And he said, 70% is to guarantee-- it is to underwrite our reputation as a guarantor, thinking mostly of Europe -- that if we didn't defend Vietnam, they wouldn’t didn't we'd defend the Federal Republic of Germany, or France.

And so you could see at that point this idea of commitment and reputation becomes all-central, even on the non-nuclear conflict. The reason is that even a non-nuclear event can affect your nuclear reputation. And therefore, you're willing to fight a substantial war like Vietnam mostly for that reason, rather than to stop China, or the Domino Theory, or to promote democracy. Those were the other 30%. But the 70% was just for the reputation of credibility as a guarantor.

You had these very odd things that came out of the doctrinal understanding of effective nuclear weapons. And one of them is called the rationality of irrationality: that it can pay to look really irrational. Herman Kahn had a phrase that in crisis, you can announce that one of us has to be reasonable, and it's not going to be me.

And the idea is that, of course, that if you are willing to say that the United States-- if the United States is willing to say that we'll defend Berlin as if it were Chicago, that's not very credible on its face. You've got all kinds of things, like go to Berlin and say, "Ich bin ein Berliner," as Kennedy did, to kind of establish that you are serious about it and that you were linking your reputation to it.

And Nixon was famous for suggesting to North Vietnam that he was irrational and that he might bomb them over, and over, and over again unless they came to the negotiating table. And he wasn't being reasonable.

So this idea of rocking the boat as a tactic is important. It might still be relevant to cyber, that one could maintain some credibility of a commitment by using cyber means to make things that are not necessarily troublesome in themselves, but that open up the possibility of things will get out of control. And that's the rationale of irrationality.

The third lesson is that more always isn't always better. And let me give you a very particular example of this, and then think about cyber analogies. The example is MIRV, multiple independently targetable reentry vehicles. In the '70s, the United States developed this technology. We could put 10 warheads on a missile, and aim them in several different directions. Then for example, if you used three or four for each target, you'd be pretty sure to knock out that missile. And you can knock out three missiles pretty reliably, with one missile.

Well, that makes for an unstable world. But the United States at the time said, gee, this is a great technology. It's militarily effective. And we've got a several year lead on the Soviets. So of course we're going to build it. And we did. And then of course, they built it. And then we both decided that things were unstable. There's more of a first strike advantage than there used to be once both sides had MIRV.

And of course, with MIRV, it's very hard to inspect afterwards. It can be done, but it's really hard. You have basically unscrew the top and look inside.

Whereas, what we could have done is said, we won't test it if you don't test it. Because the testing is really easy to observe. The radar just sees that things are splitting off of the warhead. And so we could have done that.

And Kissinger, in retrospect, said he got it wrong. He took the military's standard view that it was a better capability, and we had a lead. So we'll get it. Whereas in retrospect, it would've been a safer world had we restrained ourselves.

And there are interesting questions about cyber restraint. One example is the financial targets. But they're probably others where restraint would be useful. And so it's not necessarily that you go for the best capabilities, because sometimes those could do harm than good.

The fourth lesson is that it matters how you assign tasks to organizations. And most of you are very familiar that with from the Defense Department. But to take an example from the nuclear world, when the Air Force first got the nuclear assignment, its leadership was pilots. And their attitude toward the idea that you should put a missile in the ground and surround it with concrete was that real men don't cower in holes.

It took Wohlstetter about a thousand briefings to overcome that attitude, which is very understandable. But you can see how it's completely wrong. The assignment to Air Force, which was run by former pilots, would suggest that that would be an attitude that really needed to be overcome.

And the Navy, interestingly enough, said to the Air Force, “nuclear weapons are immoral”. They kill lots of civilians indiscriminately. They're immoral. So we don't want any part of it. Well, then they got nuclear submarines. And they changed their minds. So as soon as they got part of the assignment, they decided that this was effective war fighting strategy.

So the current issues, of which there are many in cyber, one is about whether CyberCom should be a separate command instead of being under the Strategic Command. Another issue is about integration with regional commands-- I mentioned the delegation of authority. And there are issues of allocation of responsibilities between the public sector and the private sector. These issues about organizational arrangements matter, even though they sometimes thought of as kind of irrelevant. But it’s not just a matter how many resources you allocate. It also matters in where you put them in terms of what the self-image of that organization is and what they're trying to achieve, and the career patterns of the people who run them. For example, giving something to DARPA makes it much more likely to explore unusual possibilities.

The fifth lesson is that competition can be largely over prestige. A surprising thing from the Cold War is that the nuclear competition was largely symbolic. And let me give you a couple of examples. One was that John Kennedy ran against Nixon on the idea that there was a missile gap, that we had fewer missiles than the Soviets. Well, it didn't really matter exactly how many each side had. And it turned out we didn't have a missile gap.

And so an interesting question is, what's the equivalent in the cyber world to an arms race in nuclear world? The arms race in nuclear affairs was mainly about numbers. It turned out after a few hundred, doesn't matter. But we still got to 10,000 anyway.

Prestige is what that's about. And to take another example from the Cold War period, the Russians put up the first artificial satellite, Sputnik. Big mistake. Because what it got us is science education and DARPA. So we were scared. We thought this meant that they were ahead of us in the ways that we couldn't tolerate, and that we were to make big investments in long term solutions for this. But that's a prestige thing. The satellite didn't, by itself, do anything.

Interestingly, China has chosen not to engage in a nuclear arms race. They haven't raced ahead and bought as many nukes as they could, by any means. And they basically bought enough to have a secure second strike of a small scale, but not trying in any way to make that an arena of competition. So they're finding other domains in which to compete with the United States for prestige, but they've deliberately decided not to do that.

An interesting question is about cyber. Will cyber become a domain of prestige?

So you see, for example, that wants jet planes. Peru doesn't need jet planes. None of their security threats involve jet planes. But they're really great at flybys for National Day celebrations. It's a sign that they're a grown up country. They're not the Dominican Republic. They've got jet planes.

Aircraft carriers have to some extent taken that role as the big symbols. And China is, of course, building some aircraft carriers. There's some great different opinion about whether that's a smart or dumb thing to do. The dumb version says: if they want to spend a billion dollars and put it in one place so we can sink it on the first day, that's great. More power to them. But of course, short of all out war, carriers do provide a way of projecting power. But they also provide what countries like Brazil and France already have, which is a symbol of national power.

In contrast, cyber capabilities are really difficult to use as symbols of national power, because there's not anything you could point to like an aircraft carrier or a jet plane flying by. What you can point to is demonstrated capabilities, like Stuxnet. And whether that becomes a kind of a prestigious race to demonstrate capabilities hasn't happened yet. But it could. And it could be largely about symbolic things, and not necessarily about actual practical things.

Let me come back to questions of attribution if I have time at the end.

Lesson six is that effects can cross scale boundaries. By that I mean, to take the example of the nuclear world, that nukes made the world safe for small wars. So we don't have major wars, or medium size wars between the great powers. But we have a lot of small wars-- Korea, Afghanistan, Vietnam, and many others.

And it's partly because the deterrence at the level of escalation to a major war is so likely to become nuclear that countries feel that they can fight these medium size wars without risking their national security in ultimate ways. And so in a way, nuclear weapons and technology have made the world safe for smaller wars.

And cyber has this capacity as well, because it can be tuned to any level. It could, for example, be used for signaling. So now one of the ways we do signaling is we move aircraft carriers around. When we wanted to tell the Chinese not to intimidate Taiwan with missile tests, we sent an aircraft carrier to the Straits of Taiwan. It was clearly symbolic. The aircraft carrier wasn't likely to be flying any combat missions. But it was meant as a demonstration of our seriousness. And it was seen. And attended to. And the Chinese responded the way we hoped they would.

And we could imagine using cyber technology for this kind of purpose, turn out the lights in one city to say we're really serious about something, or many other forms of the use of cyber as signaling. Not so much as capacity to actually do some harm, but as a way of signaling a concern and intent, short of use of force.

Lesson seven is that there can be a surprising amount of restraint in both the deployment and use of capabilities. To start with, there has been an amazing restraint on proliferation. We still worry a lot about it. But if you were standing in 1962 and projecting 20 years ahead, you'd expect 25 countries to have nuclear weapons by 1982. And a perfectly reasonable guess. You can list all the ones that you might think.

But it didn't happen that way. It's true that you already had the United States, and Britain, France, and Soviet Union. And then you got China, Israel, India, Pakistan, and North Korea. But that's it.

It didn't go to 25 countries. It went to 9. And even that took 40 years, but 20. So there's been actually quite a lot a restraint on the nuclear side.

But on the other hand, there's a market for the proliferation. So as you know, the Pakistani physicist A. Q. Khan sold nuclear weapons technology to Libya.

And in cyber world, one could imagine mercenaries and marketing. For example, if Malaysia wanted to pester Singapore, and they wanted to do it with cyber means, they don't have to develop the cyber means internally. They can go hire somebody to pester Singapore.

And that's a capability that is relatively new and unused. Certainly mercenaries are common in history, and they've been widely used for small purposes ever since. But the cyber opens up possibilities of rental, renting capacity, rather than buying capacity. And that's scary.

But in terms of nuclear, actually the arms race, with the exception of India and Pakistan, which are in sort of an arms race, it's been pretty passive. And the really striking thing is that when the Soviet Union collapsed, all the republics gave their weapons to Russia. Ukraine might have thought that was a mistake. Maybe they wish they still had them. But they all gave them up. And so there's an example where the restraint was really very great.

And the reason they gave them up was because the West said to Ukraine, if you want to be treated like a normal country in terms of trade relations and everything else, you've got to give up your nukes. And they thought it was worth it.

We've also been restrained on actions in the nuclear world. And a good example is the incidents at sea where the United States and Russian, and Soviet ships used to bump into each other and cause dangerous accidents. And we're now trying to do the same thing in Syria, kind of deconflict the situation. And whether we could do more of that in the norms world remains to be seen, but it's certainly a possibility.

We got very stylized in some ways. Like if we expelled three Soviet spies, they would expel three Americans. And then we'd stop. We wouldn't respond to that. And so it became very much of a stylized tit for tat in that particular domain. So there are possibilities of establishing norms, and patterns of behavior, and rules of the road that could be helpful in cyber, and that have a successful history in the nuclear world.

Lesson eight is that Track II diplomacy can be very helpful. Track II is unofficial diplomacy where maybe academics or retired military and security people talk to their counterparts. In the Cold War, there was a lot of this going on. I took part in one of them, the National Academy of Science's Committee on International Security and Arms Control talked to Soviet scientists from their Academy of Sciences and some of their retired generals. And I think they learned a good deal about how we saw stability issues as essential to the peace of the world, whereas they were much less concerned with stability and much more with sort of the balance of power.

And we learned from them. Here's an interesting example. We thought, wouldn't it be nice if we had an agreement not to attack in a conventional war nuclear power plants, because they make a mess. And what the Russian told us back was, let's not just have an understanding, let's have a treaty. Because if we have a treaty that says we won't do it, our military will put that language into their doctrine, and into their formal commands, and they won't attack an atomic power plant. But if you just say it's an understanding that we're not going to do it, the military doesn't feel quite as compelled to make sure that it never happens.

So we both learned some things about this. And of course, there's a lot of this kind of activity in the cyber world. Some of it's track 1 and 1/2, because China doesn't wants the people that talk to the United States informally about these things to be responsible people. So they tend not to be retired or academic. They're often people that are still in important positions. So it's kind of track 1 and 1/2. That kind of thing could be useful.

And there's a great deal of discussion, kind of in the open between security experts and the security community, of academics and elsewhere around the world, that are helping to shape how we see the cyber world.

I came up with a few more lessons besides the eight I had promised. The ninth is that engaging the public is really hard. So in the atomic era, the government of various countries tried to get the public involved in civil defense on the theory that if they learned about how to evacuate a city, or at least stay in the basement, you could have half as many casualties. And you could still see signs around town, 180 people in this building.

But it was a flop. The public just didn't want to have any part of it. And I think that the effort on computer hygiene as an approach to computer security has some of the same characteristics. It's very hard to get the public totally engaged in that, especially before there's a major conflict.

Lesson ten is that the way we frame issues can dramatically change when there's a major event that gives reality to it. And so of course, Hiroshima is the paradigmatic example. If we had blown off the top of a mountain as some scientists proposed, I think it would not have been as impressive and as scary for the next 40 years as bombing a city, where the effects of it were so vivid.

So if we ever have a serious cyber conflict where the effects are large, people would be very anxious to close those barn doors, not only in terms of the security, but in terms of what would set it off, and kind of make inferences about doctrine, and lessons, and what works, and what doesn't. And there would be a very fast competition for what are the lessons. And they'll make a big difference that even the minor stuff we've had so far (like in Georgia or Ukraine, or with Stuxnet and the Sony hack) just begins to scratch the surface.

But all that's small potatoes compared to what could happen. It could very likely make a very big change.

The eleventh and last lesson I want to leave you with is that even great powers are hard to predict. This is a very unfortunate and frustrating thing. Take the Cuban Missile Crisis. The CIA was asked if the Russians were going to put nuclear missiles into Cuba. And they did a serious analysis. And they said, no, because it would be totally inconsistent with their previous behavior; they had never even put them in Poland. Well, obviously *that* conclusion about Cuba was wrong.

An even better example is the start of the Korea War. Before the North Koreans invaded the South in June 1950, they had listened carefully to the American foreign policy statement of Dean Acheson four months earlier, in February1950. That official statement said that we have a defense perimeter. It runs from Japan to the Philippines. And countries beyond that, which clearly included South Korea, will have to take care of themselves. We had no commitment. The idea for that was from MacArthur, that you don't want to be defending something that's way out in the distance and not very valuable. It's just a silly way to have a defense perimeter. And we're going to tell them what our defense perimeter is.

And of course, Stalin and Mao signed off on this invasion, figuring the United States said they didn't care what happens in Korea. When Truman heard of the invasion, he was in Independence, Missouri. And he got on the plane to Washington. And before he got off the plane, he decided that this couldn't stand, that this was like Munich. That if Soviets were allowed to sponsor an attack on South Korea, and we didn't do anything, the next thing you know they'll be after Turkey or someplace else. And then it'll just escalate one after another until you stop them. You might as well stop them at the beginning, even if it's not a very important place.

And so he completely reversed the policy. So the United States intervened, even after essentially promising we wouldn't. So we're very unpredictable.

And in fact, if Truman had thought about it in February, and if somebody had said, well, if you issue this statement, they're very likely do it: to take it if you tell them that they can have it. And then wouldn't you wish you had never said it? And the answer might have been yeah, I guess we shouldn't say it, if, in fact, that's how we're going to react. But we were totally inconsistent, because we framed the issue in two different ways-- once in February about defense parameters, and then once in June about Hitler.

And so even great powers like us, or the Soviets, or others are often very hard to predict. And in terms of cyber behavior, this can certainly add to the difficulties. And one advantage of the uncertainty in the cyber world is that we get deterrence value out of the fact that we have very little confidence in our own cyber capabilities, or anybody else's.

So if the President says, if I get in a war with China, can we shut down the Chinese air defense system? I don't know what the Air Force or CyberCom would say. But they might say, we think we can do it. And the President says, yeah, but how sure are you? And they say, we don't know. We've never taken out a whole province, for example. And if we did, they would fix it. So we didn’t want to do that. So could we take out their entire air defense? Yeah, maybe, or maybe not. In other words, the day after we try our hardest, it could be at 1% of its previous effectiveness, of 99% of its previous effectiveness. We just aren't sure which.

That's great for deterrence, because it means countries can't trust their cyber capabilities.

Nuclear technology was very different. What you know for sure is that a missile would be able to take off with 90% reliability, and the bomb would explode with more than 90% probability. And it would do a megaton of damage. And all of that is pretty straightforward. The uncertainty is small, at least at that gross level. Whereas cyber, the uncertainty is very large, at least until we get major events.

That's good news and bad news. The good news is that kind of uncertainty does help deterrence. So even a hungry power that is unsatisfied with the status quo is very uncertain about what it can do. But, remember, Japan attacked Pearl Harbor. Japan knew that the United States had seven times the industrial potential. Very good estimate, they got it right. They did not do war gaming about what would happen six months later, except that they might run out of oil. So they wanted to grab everything in six months.

But apparently-- and I've looked at this in great detail-- they assumed that the United States would let bygones be bygones because we would have to give priority to Europe. Well, they were right, we gave priority to Europe. But we did not let bygones be bygones. In fact, we had a very vengeful response to Pearl Harbor. They're not going to get away with that. So they didn't predict us at all correctly.

So I think we have a variety of experiences, mostly from the Cold War that I've talked about, that give us a set of things that are possible that you're better off not using-- not developing MIRV until the other side. And we’ve learned things like how important prestige is, and how much the competition over military things is often competition over prestige in symbolic ways.

When we discovered that Khrushchev put missiles in Cuba, the first thing Kennedy asked his people was, “Are you sure?” And they showed him the photos. “Yeah, we're sure those are nuclear capable missiles.” The second thing he did was to ask McNamara, so what difference does that make? And McNamara's answer was that it doesn't matter whether a nuclear missile is launched from Russia or from Cuba.

And the President said, OK. But I have said the gravest issues would arise if they put offensive missiles in Cuba. And they did. So therefore I am committed to act.

And so again, it was about commitment rather than flexibility. What we'll need to work out with the cyber world are what are the relevant ideas, some of which may be very different from our standard understandings of military weapons and strategy.