Intro

Good morning, and thanks to Dr. Hicks and Dr. Green for the invitation to speak with you today.

I’m afraid that I have a bit of a heavy lift this morning...hope you had your morning coffee...

Want to cover three things, and then get to your questions:

● How changes in strategic environment affect deterrence;
● How the Navy contributes; and
● Key questions we face.

For better or worse, I have more questions than answers...

Strategic Environment

Let’s start with the strategic environment. I’ve argued that in many ways, we’ve not been in a competitive situation for about 25 years, and now we are back in the game
Since we’ve been gone, the game has become faster paced, more complex, increasingly competitive.

Time: unforgiving characteristic. One word to describe the pace -- exponential.

The dimension of time is very pertinent to business in the gray zone...gray zone approaches operate over time. Like the force of gravity or the shaping action of ocean waves. By definition not abrupt...

Playing out on the seas:

- Megacities expected to grow from 31 to 41 by 2030, vast majority within 100 miles of coastline.
- 400% increase in maritime traffic over the last 25 years.
- Aquaculture production increasing 13-fold in the same time.
- Tapping into undersea resources -- 99% intercontinental telecommunications runs along undersea cables.

Changes are shifting the character of naval competition/warfare and are being exploited by our competitors:
● **China and Russia**: both are able to complete on a global scale, across all domains, and possess considerable space, cyber, and nuclear forces.

● **North Korea**: relentless pursuit of nuclear-capable missiles continues to destabilize north Asia and the world.

● **Iran**: growing naval forces routinely demonstrate provocative behavior in the Straits of Hormuz, Arabian Gulf, and beyond.

● **Terrorist groups**: some supported by Iran, firing missiles and smuggling weapons.

In deterrence context, some things same, some changing.

Essence of deterrence remains credible ability to inflict unacceptable cost -- a punishment.

● In Kissinger’s formula, it’s three parts: power, the will to use it, and an adversary’s understanding of that.

● My role in this equation is to deliver on the power and understanding parts, and to support policymakers’ decisions on the will part.

● Delivering on my two pieces requires us to have clear understanding of our areas of advantage relative to others’.
● This happening in more dimension than before - I’ll talk to five
● These five dimensions - like five spices - can combine together
to form a tailored blend, depending on how hot you like your meal...

Many aspects of that are changing since we last thought about deterrence in a truly competitive context. We’re just getting started to rekindle this thinking.

Our rivals have been thinking about it the whole time…

Will run quickly through five spices of military competition and how they’re shifting:
Not cinnamon, fennel, pepper, anise, and cloves
Our five spices are nuclear, chem/bio, cyber, space, and conventional
Sounds like cooking in doctor evil’s kitchen...

**First Nuke**: still only military capability where loser can destroy the winner.
• Means we MUST maintain ability to strike back at any who pose existential nuclear threat to homeland.
• NPR focused on capabilities we need to do this -- triad remains foundation of our military strength.
• But much changing here -- more seeking to join the club.
• Some with low technology - dirty bombs, small scale, relatively simple.
• Some with advanced technologies -- smaller, more precise nuclear weapons blurring line between nuke and conventional.
• As line erodes, are we entering an era where nukes, at least of some limited size, could be seen as acceptable?
• Can we deter in this area if we don’t get engaged in this type of research? Understand these advanced weapons? Does this asymmetry prevent effective deterrent posture?

Second: Chem/bio: remains an attractive option for those who see few other areas where they can gain an upper hand.
• Advances in biotech make threat more potent and more likely as science spreads.
• Particular challenge because of attractiveness to weak states and non-state actors -- hard to determine what they value.

• I’m not an expert, but seems super hard to control.
  ○ Like gas attacks...the wind may blow back on you!
  ○ There’s a reason that the word “viral” seizes and holds the mind...

**Third: Cyber**: the other “viral…”

• Report by Defense Science Board concludes others’ offensive capabilities likely to far exceed our ability to defend critical infrastructure for at least the next 5-10 years.

• Also clarifies need to deter **attacks**
  ○ Stuxnet, but also Ransomware

• And costly **intrusions**
  ○ Theft of intellectual property and political manipulation.

• Low barriers to entry, high degree of military and commercial reliance, challenges with attribution make this one of most attractive planes of attack.

• Recent history bears this out
  ○ Is there a cyber “gray zone?”
• “Target” in many of these incursions / attacks seem to be the confidence of the institution...can they be relied upon to portray the real truth? Protect their assets (which may be MY assets!!)?

• Cyber is perhaps most obvious area that illustrates need to consider not just relative advantage within context of single strand capability - like cyber - but to integrate across several of them.
Fourth: Space:

- Also poses unique challenges -- commingling of different kinds of military signals, or of collateral damage to important civilian capabilities if military actions are taken -- make responding in kind to space attacks very complex.
- As in cyber, clear and shared understanding of what constitutes an attack is a critical element of any deterrence effort -- more complex than in some other areas. Much like gray zone...an ambiguity emerges...
- Competition absolutely heating up here, becoming more complicated as mini- and microsats proliferate, commercial launches become much more frequent.
- One of biggest deterrence challenges we may face in coming years -- doesn’t lend itself to punishing “in kind” because consequences so hard to predict or contain.
- Space situation seems very fragile -- easy to lose all of what we currently have. Who benefits or loses is all of space is taken down?
- Likely area where lines need to be as clearly drawn as possible, and harm inflicted in other venues. UNCLOWeb
Conventional: Trends here are staggering.

- Era of competition for precision giving way to era of competition for decision.
  - Our advantage was historically in our ability to observe and orient -- as satellites and sensors proliferate, playing field is leveling.
  - Shifting the competition to orient and decide -- if everyone can observe, who is quickest to figure out what matters and decide what to do about it?
- Information warfare -- including data analytics, big data, and related, deception -- at the center of this.
- Technologies like autonomy and artificial intelligence challenging not just laws and policies, but perhaps more significantly, our culture.
- Again, have to advance the conversation as quickly as we can, but also be clear-eyed about what we might be willing to do relative to some of our potential adversaries.
- Need some serious game theorists to test this out...I’m hiring...
• Conventional realm remains highly relevant in maritime context -- navies around the world are booming, as some hope to expand their maritime influence and others seek to respond to growth.
Brings us to **gray zone**:

- Increasing reliance on these approaches logical for those who want to avoid our strengths, and believe we are not well postured to respond.
- Transparency and democracy may make us vulnerable, but also our greatest strength.
- Requires way of thinking and collaboration that is hard with our current structure -- must adapt.
- Largely concur with CSIS recommendations:
  - To work, deterrence needs to be tailored to the situation;
  - A unique “blend” of some or all of the five spices for the situation at hand
- Remember the dimension of time...some of these gray zone effects manifested over a longer time…
  - How do you deter the frog from entering the pot?
  - Or the cook from turning on the heat to start the water simmering?
- What exactly are you trying to prevent?
- Is deterrence even desirable in the gray zone?
So many of the new domains seem “all or nothing” in their nature (chem bio, space).

Is a gray zone “outlet” desirable or even necessary to provide a venue to show a willingness to act in ways that are not catastrophic?

- Alliances are important, when ally is subject to coercion and is willing to partner closely with U.S. then U.S. should tighten the alliance
  - Gray zone often involves a violation of international conventions, laws, norms, that govern a commons
  - International pressure to maintain order in that commons will be more effective than one nation acting alone...

- U.S. will need to accept more risk, or maybe less risk? than it has in the past to effectively deter coercion.
How the Navy Contributes

Navy plays key role in all of the areas above.

Ensuring military ways to punish are credible:

- COLUMBIA -- Navy’s contribution to ensuring undersea leg of nuclear deterrent remains most survivable, uninterrupted;
- But by being forward and present -- all over the world;
  - Uniquely responsive if crisis erupts - first to arrive; deter bad behavior, hooligans and shenanigans...
- Also present and persistent over time -- also enables assurance and deterrence - shaping thinking. Operates on the same time scale as gray zone tactics...a counter-narrative;
  - Conducting FONOPs all over the world to demonstrate commitment to upholding international norms and laws.
- If deterrence fails, and we enter conflict, Navy a key contributor to military operations - we see this today;

Denying benefits others might be seeking (changing their cost-benefit calculations):
• Adding to lethality of our current platforms and fleet more generally to keep pace with adversary advances in conventional context; and
• Cyber teams developing offensive tools for both national and operational use.
• Enhancing cyber resilience, increasing training to fight through network degradation.
• Contributing to joint force efforts to increase space resilience.
Key Questions We Face

What should we take away from this quick review?

Deterrence, like rest of the environment, growing increasingly complex -- as CSIS report describes, overall strategy has to simultaneously solve a “rubik’s cube” of three sets of variables:

● Deterrent mix of the five spices must be carefully thought out…
  ○ Consider like-on-like when appropriate
  ○ Respond through other means when required.
  ○ Tailored to specific actors
  ○ But at the same time hold together across the whole
  ○ All other actors will be watching what we do...to one

● Approaches must be informed by very solid strategic intelligence about what the other side values -- huge task for the IC.

● High-end competitors able to pose unique challenges using all five spices, and also gray zone approaches.

● Low-end competitors also work gray zone approaches and Chem-Bio, growing ability to leverage cyber.

● Needs to signal our choices about
○ punishment or denial
○ specificity of commitments
○ implications for allies
○ our tolerance for risk.

A bunch of interesting and important questions:

● If speed is today’s dominant characteristic, how does this affect deterrence? Deterrence doesn’t seem to benefit from speed...
● Different in different avenues -- cyber moves at speed of light and bytes, but survivable second strike in nuclear context slows things down a bit and BUYS time that we wouldn’t have in a solely land-based missile exchange.
  ○ Is there a “second strike” possible in cyber? Space?
● In all or nothing scenarios (MAD scenarios) who has more to lose if it all goes away?
  ○ If we have more to lose than many others in those domains, how does this affect our deterrence calculus?
● As technology makes small nuclear or EMP weapons feasible, what effect, if any, does this have on our nuclear deterrence strategy?
What are the limits of deterrence for weak or non-state actors? Hugely complicated task, and one that technological advances and spread complicate still further every day. How do we deter weak states and/or non-state groups?

Defense Department tackling these questions this summer, so CSIS efforts perfectly timed to help us think them through.

Making a real contribution to perhaps our greatest need -- a community of committed, high quality thinkers to rejuvenate robust debate and scholarship around these deterrence questions.

All of you here today are a part of that too, and hope that you’ll continue to stay engaged and bring others into these critical conversations.

Thanks, look forward to your questions.