The Null Hypothesis

1. To wit: the state of U.S. deterrence is adequate – and no set of solutions can improve on the present situation without creating greater offsetting costs and risks.

2. The United States already has an implicit deterrence policy (plus some explicit comments on this policy via the 2011 International Strategy and the 2015 DoD Strategy). Pearl Harbor and 9/11 say that a response kicks in when deaths exceed 2,000 (and possibly lower). At that point, the country perceives an existential threat and reacts accordingly.

3. Adding certainty to a deterrence policy has costs:
    a. It may commit the United States to undertake retaliation in situations when the costs of doing so may exceed the benefits of doing so.
    b. It may induce other countries (e.g., China) to declare their own deterrence policies thereby raising the risk of instability arising from action-reaction cycles
        i. It hardly helps that other countries have very poor attribution capabilities but may have to pretend otherwise.

4. Deterrence-by-punishment has several components, which are hard to improve
    a. Attribution – we think we have pretty good distribution, but it has two problems:
        i. It has been good against those who really don't care much if they are fingered (or may even want to be).
        ii. We refuse to display enough of our evidence to be convincing to even potentially friendly third parties. This will matter if the retaliation is nontrivial.
    b. Thresholds – we keep making this up as we go along. In the case of Iran and the DPRK we had much bigger issues among us (e.g., their nuclear program, the threat to the south) than the modest amounts of damage each caused us in cyberspace.
    c. Will - The DPRK non-response did not help. We may not be able to credibly give evidence of our will absent an actual response. Even then that will be a context-limited single data point.
    d. Capability - This is the least of our problems after Stuxnet and Snowden (as long as the attacker has something of value at risk from cyberattack, which the DPRK may lack).
    e. Legitimacy will be an issue in determining whether the attacker folds or raises.

5. Deterrence-by-denial
    a. The most important element may be to frustrate the reason that countries carry out attacks on the United States. Many expect an aversion or a goading response or just want attention. Shrugging off an attack may, in such cases, be the best strategy but one incompatible with a declared deterrence policy.
    b. Improving resilience is great, but whether it adds to deterrence depends on:
        i. Whether they see the results.
        ii. Whether the demonstration makes them:
            1. Wonder why we needed to do it (SecDef Cohen and Anthrax)
            2. Wonder if we are gearing up to something on the principle that we project what they can do to us from what we can do to them
    c. What *does* matter is that they cannot carry out a first strike against our conventional forces in the hope that they can move while we are still confused. But the way to demonstrate resilience may entail not proving that our systems can survive a cyberattack, but that our military can function unimpeded even if systems fail