Questions for the Record
Senator Dianne Feinstein

Crime and Terrorism Subcommittee Hearing On:
"The Modus Operandi and Toolbox of Russia and other Autocracies for Undermining Democracies Throughout the World"
March 15, 2017

Questions for Ben Buchanan

1. In an October 2016 report about cyber threats to our elections, you argued that Russia, in particular, has "plausible motivations and capabilities for some kinds of electoral interference."
    a. **Could you provide us with some key details about what those motivations and capabilities are?**
    The Intelligence Community's declassified reports provide excellent insight into the capabilities and motivations of Russian operators. The community concludes that the Russians had a specific interest in benefitting one candidate in the election, not just in causing general disruption. Further, the community notes the variety of mechanisms through which the Russians carried out their activities, including hacking and propaganda operations. In addition, I recommend reading the testimony of Thomas Rid before the Senate Intelligence Committee on March 30th, 2017, which did a very good job of summarizing public evidence of Russian operations. I find that the community report and Professor Rid's testimony align very well with what I have observed.

    b. **What are the areas of greatest vulnerability for the US?**
    I often say that when it comes to cyber offense, the United States has the nicest rocks, but when it comes to cyber defense, we live in the glassiest house. It is important for us to increase the baseline standard of cyber defense in order to better guard against intrusions. This is especially true when it comes to critical infrastructure, such as the electric grid, water systems, voting machines, and more. Failure in those areas represent real threats to Americans. It is also true of government networks that store vital information, as the breach at the Office of Personnel Management demonstrated.

    c. **What steps should the US be taking to address these problems**?
    At a minimum, we should seek to raise the cost of actions for our adversaries. At an individual level, it is essential to take basic cybersecurity precautions. These include the use of two factor authentication and a password manager. At a government level, it involves replacing legacy systems with ones designed with a security focus, and, more broadly, modernizing IT capabilities in the federal government. To this end, President Obama's proposed federal network modernization actions would represent a good start if enacted.

2. In the same report, you also warned that our "voting infrastructure" has not "been designed with cybersecurity as a priority." And in a December 2016 paper about Russian cyber operations, you argued that "while electoral influence in general is not new…it is deeply unusual for the United States to be on the receiving end of it."

   a. **What should we be doing to better address vulnerabilities in our voting infrastructure?**
   Elections in the United States are not federally run, and I do not believe that should change. However, there is likely a role for the federal government to play in supporting state and local entities in their election work. This might take a form similar to the Help America Vote Act of 2002, which provided money to replace outdated voting machines and helped raise standards.

   I have written in a more detail fashion about election cybersecurity in a paper (with Michael Sulmeyer) entitled "Hacking Chads." Four areas of possible improvement in American elections discussed in more detail in that paper are:
   - Better security audits of voting infrastructure prior to the elections themselves. California and Virginia provide strong examples of the importance of this sort of work.
   - Ensuring that there is a voter-verified paper trail. Most states do this, but some do not. A lack of a paper trail makes tracking and correcting irregularities much harder.
   - Instituting risk-limiting post-election audits. These audits verify, with a high degree of statistical certainty, that interference did not change the outcome of an election. Audit procedures currently vary enormously by state.
   - Enacting a declaratory policy in which the United States promises to respond to foreign interference in its elections. This is necessary in order to establish some kind of deterrent.

   b. **How would you respond to those who claim that Russia's interference in our 2016 election is just another example of its attempts to meddle in our affairs – and therefore somehow less problematic or pressing?**
   While Russian interference may go beyond just election interference, that in no way diminishes the significance of the election interference itself. Elections are fundamental to democracy, and any attempt to meddle in them deserves scrutiny and resistance. I think the Russian activity from 2016 is both problematic and pressing.