




(Bennett Craig)

An overflow crowd listens to a panel discussion on the background and impact of Russian cyber attacks.

 **NEWSLETTER ARTICLE** – *Belfer Center for Science and International Affairs, Harvard Kennedy School Belfer Center Newsletter*

Russian Cyber Operations 2017

Spring 2017

Featured Event: “Russian Cyber Operations: 2017 and Beyond” February 1, 2017, Harvard Kennedy School

As Russia’s alleged cyber-intrusions into U.S. affairs continue to grab headlines, the Belfer Center’s Cyber Security Project convened a panel of experts in February to discuss Russia, cyber security, and the intersection of the two. Speakers at the event included experts and authors David Sanger, chief Washington correspondent for The New York Times and senior fellow at the Belfer Center, Fiona Hill, named in March as NSC senior director for Europe and Asia and a Center alumna, and Ben Buchanan, fellow at the Belfer Center’s Cyber Security Project. Michael Sulmeyer, director of the Cyber Project, moderated the overflow event.

Following are paraphrased comments:

What do we know about Russian hacking?

Ben Buchanan: Russian cyber hacking goes back a long way, to the “Moonlight Maze” case in the 1990s....The Russians recognize the power of cyber operations, not just to steal information but also to attack.

Fiona Hill: What is unusual is the backdrop of an American election process with unprecedented efforts by Russia to have influence in it.... With a few taps of computer keys, rather than physical action, you can start to shape events.

David Sanger: Timing of the leaks seemed strategic: The first public release of the hacked information came just before the DNC national convention and resulted in a high-level resignation; the next release came within hours after the news about then-candidate Donald Trump saying some fairly crude things. These leaks first came over two channels that we believe the Russians themselves set up and, when those weren't getting enough clicks, the materials went to WikiLeaks.

BB: Cyber operations intersect quite neatly with information operations, propaganda and what the KGB called "active measures," including false information.

FH: Putin is a former KGB operative...and extols the virtues of the techniques he mastered in the KGB, and their application to politics.

DS: In Putin's mind...Hillary Clinton interfered in Russian elections in 2011-12.

Should the U.S. have reacted differently?

DS: The intelligence community could have offered up more information and ratified much of what had already been brought to light by private companies.

BB: This is a dilemma for the intelligence community: When should they piggyback on the private sector and when should they fear what it will say?

FH: When it comes to a "proportional response," you have to tread very carefully.

DS: Had we called out Russia and applied sanctions right in October, it would have invited them to come in and mess around with the election infrastructure... on Election Day. So the U.S. didn't want to go up the escalation ladder.

Will Russia continue its cyber attacks on the U.S. and elsewhere?

FH: I think we will see more cyberattacks as agencies in Russia try to prove their worth. Russia also has a presidential election coming up, in 2018, and Putin has to put himself up for "relegitimation."

BB: Russian attempts at cyber-interventions in other countries' elections are not likely to stop. Europeans are concerned, especially in countries where elections are coming up....The question is: What are they going to do about it?....This story is not going away.

For more information on this publication: Please contact the [Belfer Communications Office](#)

For Academic Citation: "Russian Cyber Operations 2017." Belfer Center Newsletter. Belfer Center for Science and International Affairs, Harvard Kennedy School. (Spring 2017).