UNIVERSITY OF MARYLAND GLOBAL CAMPUS
Formerly UMUC | Global Media Center

# Cyber Threats Are Testing Liberal Democracies, Says NSA's Barnes

Posted on January 29, 2020 by Gil Klein in Cybersecurity, News and tagged Cybersecurity, Events, Featured, News, Top News.

The United States and its democratic allies are in a struggle with autocratic powers that are using cyberattacks to undermine elections and to steal technology secrets as well as money to underwrite their regimes, said George Barnes, the deputy director of the National Security Agency, in his Jan. 21 address to the Maryland Cybersecurity Council.

Yet getting all 50 states to work together to stop attacks on the 2020 elections is proving to be difficult, even after cyber incursions into the 2016 and 2018 elections became obvious.

“Our No. 1 priority is the 2020 elections, [but] we found it is not easy to bring 50 states together on cybersecurity” because states have differing opinions on cooperating with the federal government, Barnes said.

“Many states are very willing and able, and others say they don’t want our help. They say, ‘We want to maintain our independence.’”

He added that, though it is essential to find the balance so that “our elections are secure and trusted and verified,” it is increasingly difficult to do so. “That gets harder and harder every year because we have players on the outside of the U.S. who want to make it hard so that we wonder if what we see is reality.”

The struggle, he said, is between autocratic states led by China, Russia, North Korea and Iran that want to undermine democracy and capitalism.

“All of the countries that are presenting challenges to us are autocratic regimes. We are in a struggle to uphold the ideals on which we are founded,” Barnes said. “Our models of a liberal democracy are being tested not just in the United States, but if you look at our allied partners around the world, they are being tested in their own regions.”

In large part, this struggle is a reaction to globalization, which had been the underlying principle of international relations for decades, he said.

“Everything had become interconnected all over the world,” he said. “Now, several trends are pushing us into de-globalization. In Maryland, we are very internationally focused. But if you go into the heartland, it is not so evident.”

According to Barnes, all of Russia’s security agencies are attacking the United States simultaneously. And, though Russia itself is in a weakened state economically, he said it still poses a threat to the United States as an advanced nuclear state with a global network determined to undermine western democracies while supporting autocracies such as Venezuela.

Once the Russians figured out that we could identify attacks coming directly from them, he said they set up outposts around the world to pursue the same aims.

“They want to do things to divide our society, They will try to find chess matches between political candidates but also seek out fissures that they can widen in our society.”

But Barnes said that China poses an even greater threat. Its goal, called “Made in China 2025,” is to become the dominant producer in every major industry, even while it seeks to expand its influence worldwide through major development projects that will make other nations China-dependent.

They are doing it, he said, by stealing as many technological secrets as they can from the United States and putting “its economic model on top of ours [to] turn it inside out.”

"This all goes back to cybersecurity," Barnes said. "It is unfortunate that we have to be paranoid because if we are not paranoid we are getting rolled slowly." For example, U.S. industries that have had primacy are finding technological secrets have disappeared and dominance diminished. "You look at Chinese advanced weapons systems and you see they have a resemblance to our weapons systems."

At the same time, he said, Iran remains a regional destabilizer, as it has been since 1979. And as the United States presses it, the Iranians press back. One way it does so is through cyber operations.

North Korea wants more respect—and it wants more money, said Barnes, who explained that pressure imposed by the United States to stop North Korea from becoming nuclear-capable causes that country's regime to use cyber theft to garner the money it cannot get through normal trade and investment.

The cost of protecting our nation from cyber threats is rising quickly, he said. The U.S. must invest in people who will have the talent and know-how to jump in and provide robust cybersecurity.

**About the Maryland Cybersecurity Council**

The Maryland Cybersecurity Council is a statutory entity chaired by the Maryland Attorney General. With nearly 60 members, the Council includes federal partners (NSA, NIST), key members of the State's executive branch and other agencies, such as the State Board of Elections, members of the Maryland General Assembly, and representatives from the State at large: critical infrastructure providers, and small- and medium-size businesses, education, trade and other advocacy groups. The Council makes policy recommendations on a range of issues including critical infrastructure protection, the cybersecurity of Maryland state and local governments, and cybersecurity workforce development. By statute, the University of Maryland Global Campus is the staffing agency for the Council. More information about the Council can be found at http://www.umuc.edu/mdcybersecuritycouncil