America must defend itself against the real national security menace

Fareed Zakaria

March 9, 2017

This week, we have watched the perfect example of a country fighting the last war. The Trump administration has devoted weeks of energy and political capital to rolling out its temporary travel ban against citizens of six Muslim-majority countries, none of whom, according to the libertarian Cato Institute, have committed a single deadly terrorist attack in the United States over the past four decades. Meanwhile, the White House's response to a devastating barrage of WikiLeaks disclosures that will compromise U.S. security for years was a general vow to prosecute leakers.

The WikiLeaks revelations are designed to uncover and cripple U.S. intelligence operations of any kind, against any foe — including Russia, China, the Islamic State or al-Qaeda. WikiLeaks claims to be devoted to exposing and undermining centralized power, yet it has never revealedanything about the intelligence — or domestic policing — operations of the Russian or Chinese governments, both highly centralized dictatorships with extensive and advanced cyber-intelligence units. Indeed, WikiLeaks has chosen as its obsessive target the United States, which probably has more democratic oversight of its intelligence agencies than any other major power does.

Since the North Korean government's 2014 attacks on Sony Pictures Entertainment, many in the intelligence community, including Adm. Michael S. Rogers, have warned that "we're at a tipping point." Rogers, head of the National Security Agency and U.S. Cyber Command, testified to Congress in 2015 that the country had no adequate deterrent against cyberattacks. He and many others have argued for an offensive capacity forceful enough to dissuade future threats.

But the digital realm is a complex one, and old rules will not easily translate. The analogy that many make is to nuclear weapons. In the early Cold War, that new category of weaponry led to the doctrine of deterrence, which in turn led to arms-control negotiations and other mechanisms to foster stable, predictable relations among the world's nuclear powers.

But this won't work in the cyber realm, Joseph Nye says in an important new essay in the journal International Security. First, the goal of nuclear deterrence has been "total prevention" — to avert a single use of nuclear weapons. Cyberattacks happen all the time, everywhere. The Defense Department reports getting 10 million attacks a day. Second, there is the problem of attribution. Nye quotes defense official William Lynn, who observed in 2010, "Whereas a missile comes with a return address, a computer virus generally does not." That's why it is so easy for the Russian government to deny any involvement with the hacking against the Democratic National Committee. It is hard to establish ironclad proof of the source of any cyberattack — which is a large part of its attractiveness as an asymmetrical weapon.

Nye argues that there are four ways to deal with cyberattacks: punishment, entanglement, defense and taboos. Punishment involves retaliation, and although it is worth pursuing, both sides can play that game, and it could easily spiral out of control.

Entanglement means that if other countries were to harm the United States, their own economies would suffer. It strikes me as of limited value because there are ways to attack the United States discreetly without shooting oneself in the foot (as Russia has shown recently, and as Chinese cybertheft of intellectual property shows as well). And it certainly wouldn't deter groups such as the Islamic State, al-Qaeda or even WikiLeaks.

The other two strategies merit more consideration. Nye contends that the United States should develop a serious set of defenses, beyond simply governmental networks, that are modeled on public health. Regulations and information would encourage the private sector to follow some simple rules of "cyber hygiene" that could go a long way toward creating a secure national network. This new system of defenses should become standard in the digital world.

The final strategy Nye suggests is to develop taboos against certain forms of cyberwarfare. He points out that after the use of chemical weapons in World War I, a taboo grew around their use, was enacted into international law and has largely held for a century. Similarly, in the 1950s, many strategists saw no distinction between tactical nuclear weapons and "normal" weapons. Gradually, countries came to shun any use of nuclear weaponry, a mutual understanding that has also survived for decades. Nye recognizes that no one is going to stop using cyber-tools but believes that perhaps certain targets could be deemed off-limits, such as purely civilian equipment.

Of course, the development of such norms would involve multilateral negotiations, international forums, rules and institutions, all of which the Trump administration views as globaloney. But at least it is working hard to prevent Yemeni tourists from entering the country.