AMERICAN FOREIGN POLICY COUNCIL

We're not putting up a fight against Russia's cyber warfare

November 8, 2017 *The Hill*

Related Categories: Cybersecurity and Cyberwarfare; Intelligence and Counterintelligence; Military Innovation; Baltics; Caucasus; Central Asia; Russia ; Ukraine

Every day seems to bring fresh revelations of an ever-expanding scope of Russia's cyber and information war, not only against the U.S. but also against our allies in Europe as well.

Undoubtedly such revelations may amaze non-experts but to those who follow Russia or information warfare professionally these attacks and their scope should not have come as a surprise. As the recent Frontline series "Putin's Revenge" rightly argued, Putin began to wage war against the U.S. in 2003-04 or. More precisely it was based on worst-case thinking, that we were coming for him then.

Indeed, after the Beslan tragedy of 2004 he said as much and in early 2005, immediately after Moscow's first effort to subvert Ukraine failed, his defense minister Sergei Ivanov told the Russian General Staff Academy that, "Let us face it, there is a war against Russia under way, and it has been going on for quite a few years. No one declared war on us. There is not one country that would be in a state of war with Russia. But there are people and organizations in various countries, who take part in hostilities against the Russian Federation."

More recently, Dmitri Trenin, Director of the Moscow office of the Carnegie Endowment, observed that, for some time, "the Kremlin has been de facto operating in a war mode."

This non-kinetic war began back then and has led, via strikes against Estonia, Georgia, Ukraine and Europe, to what we have seen in the last few years. Neither should anyone think it began in 2016 with the presidential election. As homeland security expert Clint Watts noted discerning observers of Russian information warfare noted the intensification and expansion of Russian efforts by 2014. Consequently, one of the most disturbing revelations to have come out so far (and almost certainly there will be still more damaging ones to come) is just how negligent and complacent our public authorities and private establishments were with regard to the concepts of information war, cyber-security and protection of vital infrastructure, e.g. state election commissions.

Partisan political sentiment should also not obscure the gravity of these attacks or of the consequences of this unmerited complacency and neglect. Whatever readers may feel about the outcome of the presidential election last year, it should be incontestable that an attack on the integrity of our electoral process itself is as, UN Ambassador Nikki Haley, and former Vice President Dick Cheney have said, an act of war or tantamount to it.

In this context, the Obama administration cannot escape blame for failing in its most fundamental responsibility of defending the security of the United States. And as we have seen, major corporations and government agencies have also been seriously derelict in preventing cyber attacks on vital infrastructure or information. Thus millions of Equifax's credit reports were hacked and millions of civil service records were apparently hacked by China due to the OMB's carelessness.

Russian cyber warriors first were able to attack Pentagon classified systems in 2008 and since then numerous other government agencies have been hacked with apparently no retaliation. In other words, they acted with impunity.

Thus the ongoing failure of the White House to acknowledge what is now taken everywhere as fact and to address the need for a serous public-private strategy of defense, possible retaliation and protection of vital public and private networks adds the Trump administration to the lengthening list of major institutions that have fallen down on the job, starting with the Obama administration.

As long as this situation is left unchallenged, Moscow's war on the West can continue with apparent impunity we can be sure that not only Russia but other, similarly inclined actors, be they governments, terrorists or others who are just malevolently motivated, will continue and intensify their attacks on our networks. It's already time to prepare our defenses for the 2018 elections in an organized systematic way.

Writing as a war correspondent during the Balkan wars of 2012-13, Leon Trotsky memorably observed, “you may not be interested in war, but war is interested in you.” That insight aptly describes the situation we now face and the sooner we recognize that we are under systematic attack and take adequate and sufficient means to protect our networks and our democracy the less likely it is that these attacks will be anywhere near as successful or protracted as they have been. Regardless of who is president the defense of democratic processes and institutions is his or her number one responsibility. It is long since high time that President Trump, and if not he then Congress act. After all, as Lincoln memorably wrote to Congress, “We, even we hold the power and bear the responsibility.”

Stephen Blank, Ph.D., is a senior fellow at the American Foreign Policy Council. He is the author of numerous foreign policy-related articles, white papers and monographs, specifically focused on the geopolitics and geostrategy of the former Soviet Union, Russia and Eurasia. He is a former MacArthur fellow at the U.S. Army War College.
