Arcanum in the news

WARRIOR

5 WAYS AMERICA CAN DEFEND ITSELF FROM 'NONPHYSICAL' ATTACKS

October 4, 2017

By Patrick M. Cronin and Harry Krejsa

Earlier this month it was revealed that Russian-linked Facebook accounts purchased more than $100,000 in divisive political advertisements on the social network during the 2016 election. Combined with Wikileaks coordination on other Russian meddling, the campaign revealed the fragility of our exposed democratic machinery in the information age. We can safely predict that it will not be the last time foreign actors attempt to disrupt American politics, and that the Russians will not be the only ones who try.

At the same time that foreign influence threatens the very fabric of our democracy, the integrity of American commercial institutions are also under siege. Vast breaches of sensitive data have become almost routine, exposing compromising information to bad actors motivated either by politics or mere profit. The scope and scale of these challenges are difficult to fathom, but collectively they comprise forms of irregular warfare that exploit the vulnerabilities of an open society and a free market, threatening the legitimacy of both. The United States needs a multidimensional counter-offensive to brush back this new wave of attacks on American institutions.

A Chinese national flag waves in front of the former headquarters of Google China in Beijing June 2, 2011. Suspected

Chinese hackers tried to steal the passwords of hundreds of Google email account holders, including those of senior U.S. government officials, Chinese activists and journalists, the Internet company said. (Photo: Reuters/Jason Lee, 247Sports)

Contours of the Problem

It was not simply the pilfering of emails that threw the 2016 campaign into disarray. The welter of disinformation, some 3,000 ads on Facebook, the assault on back-end processes such as voter registration and local election databases, and the hacking of critical election service providers all left intolerable levels of doubt in the minds of the American electorate. New defenses against these attacks will be necessary if we are to preserve our basic rights and the integrity of our electoral system.

In the meantime, Americans will not find solace in the integrity of their digital privacy. It will take years to understand the full impact of the recent grand theft of sensitive personal, commercial and security data. This summer, Equifax, one of America's three large credit-monitoring companies, reported its failure to protect birth dates, social security numbers, and driver's license numbers for more than half of the adult population. This breach of personal information comes only a few years after Yahoo apparently had all 3 billion users' accounts hacked. Around the same period, cyber warriors linked to PLA Unit 61398 cracked into the Office of Personnel Management and gained access to 5 million fingerprints and the complete files of 4.2 million U.S. government workers. Yet the most highly sophisticated Chinese cyber espionage is said to have been undertaken by a clandestine state outfit known as Axiom, which in recent years has penetrated Fortune 500 companies, government agencies, software firms, think tanks and nongovernmental organizations.

While both nongovernmental and state actors have proven adept at stealing Americans' personal information, foreign powers are thought to be the driving force behind the large-scale intellectual property theft facing the U.S. economy. The costs of this theft is estimated to run as high as $600 billion a year. It's a vast problem involving many actors, although China is said to be responsible for 50–80 percent of the problem. A bipartisan commission led by retired Adm. Dennis Blair and former Gov. Jon Huntsman detailed the problem and outlined a comprehensive set of responses in a revised 2017 report. To compound the issue, China is not only stealing our intellectual property, but also using state-owned companies to spread strategic influence throughout Eurasia and the Indo-Pacific region as part of its Belt and Road Initiative (BRI). The initiative is making big promises, not all of which it will be able to keep; but China is likely to build more miles of highway alone by 2020 than exist throughout the entire U.S. interstate system.

In addition to robbing the United States of its innovative edge, large scale intellectual property theft also threatens the potency of our defense industrial base. If even the best defense company starting today were to design a complex weapon system, how likely is it that it would remain uncompromised by the time it became operation? Threats to our core defense programs from theft, manipulation, corruption, and degradation have never been greater than they are today, and the situation is far from under control. Major defense acquisition programs and goods and services increasingly are in jeopardy from foreign intelligence officers, terrorists, criminals and employees. With concentrated databases, one corrupt contractor can do untold damage to U.S. security.

Finally, the United States must take an expansive view toward strategy in the twenty-first century. Competitors like China are using novel tools (like cyber espionage) to shape what it views to be the future geostrategic and geo-economic battlefield. China is less to blame for pursuing its national interest than America should be scolded for squandering its security advantage. We are failing to safeguard that which is valuable and in many cases facilitating the ability of our potential adversaries to plunder our democracy and use of our strongest assets against us.

For these and other reasons, the United States requires a comprehensive response to defend the homeland from more than just physical attack. Here are five responses that might comprise the pillars of a counter-offensive.

1 - We Need a Rigorous Net Assessment of Foreign Influence

The United States needs an expansive threat assessment of internal threats and vulnerabilities, with a robust set of indicators that could measure our vulnerability over time. This ongoing endeavor would be strengthened through shared threat assessments with our closest allies and partners around the world. This assessment could help delve into everything from our exposure to digital dependence to vulnerabilities in the supply chain.

2 - We Need a Root-And-Branch Review of the Legal Framework for Protecting the United States from a Diverse Array of Foreign Influences

A combined public and private sector review is needed on how assess nefarious foreign influence over investments, real estate, cyber intrusions, political disruptions and espionage. This is bigger than reforming the Committee on Foreign Investment in the United States (CFIUS), although that is necessary. The Blair-Huntsman commission report offers short- and long-term remedies, including making intellectual property (IP) a chief criterion for CFIUS approval of foreign investments, and promoting means to identify and recover IP stolen through cyber space. Similarly, the Trump administration is to be applauded for seeking possible new trade measures to counter threats as diverse as economic cyberespionage, hostile takeovers of high-tech businesses, and unfair rules imposed on joint ventures. But the Executive and Legislative arms of government need to work in tandem on a series of legislative reforms aimed at cracking down on clandestine foreign activities, not unlike those championed by Attorney General George Brandis in Australia.

3 - We Need to Build a New Strategic Communications Capability

We have long since forgotten the art of strategic communications, even though we presently face unprecedented degrees of disinformation and propaganda. This capability should be resuscitated to so that twenty-first century democracies can withstand challenges from foreign disruption, subversion and espionage. Such strategic communications should include an offensive capacity, able to project the truth into areas where censorship prevails. Yet fighting social media ads with more social media ads ultimately will not be enough; as one astute analyst has noted, we will also need to train the foot soldiers who can take the argument the “final three feet” in face-to-face discussions.

4 - Diplomacy Should Be Used to Curb Undesirable Actions by Major Powers and Other Actors

Negotiation can help to set higher standards regarding what constitutes impermissible foreign intrusion into the affairs

and cyber domain of another state. The Obama administration started a robust but focused dialogue with China aimed at defining interest-based cyber norms. The Trump administration should determine which rules of the road are most important, negotiate enforceable standards with China and Russia as possible, and use diplomacy with allies and partners to help burnish a rules-based system.

5 - As a Prerequisite for All Other Pillars of an Effective Response, We Need a Coherent Strategic Vision

The Trump administration's first National Security Strategy, the core elements of which are currently being debated, should strive to protect American interests from a position of strength, by maintaining a balance of power and preserving U.S. competitiveness. When the strategy is completed, it should be used in part to engage close allies, so that common strategies can be forged for countering Russian influence operations, China's geostrategic and geo-economic competition and other salient challenges.

In the twenty-first century, state integrity includes far more than durable borders. These five steps are neither exhaustive nor simple, but in combination represent important initial moves to help buttress modern American sovereignty.

This story was originally published by The National Interest

Dr. Patrick M. Cronin is Senior Advisor and Senior Director of the Asia-Pacific Security Program at the Center for a New American Security (CNAS). Harry Krejsa is the Bacevich Fellow at CNAS.