Jolie Mengert

Kyle Larson

American Foreign Policy 2300

18 September 2017

Cyber Diplomacy: The United States' Weakness or Strength?

Introduction:

In a modern world completely integrated with technology, the United States' stance on cyber diplomacy has never needed to be clearer. With the recent scandal of Russia's interference with the United States' presidential election, the topic of the US's stance on cybersecurity was put into question. As a major leader of the free world, it was practically shameful that the President pushed aside the investigation on Russia hacking of the 2016 presidential election. In my opinion, it's important that the United States has a powerful yet open policy when it comes to cyber diplomacy with foreign countries.

Previous Policy:

The United States' first official attempt at cyber diplomacy started with the creation of the Office of the Coordinator for Cyber Issues (CCI) in February 2011. This branch of the government reports directly to the Office of Secretary, which is comprised of people directly underneath the Secretary of State. According to the CCI, they are a department created to "[support] international trade and commerce, [strengthen] international security, and [foster] free expression and innovation" (Office of the Coordinator for Cyber Issues). In accordance with President Obama's Cyberspace Policy Strategy, the CCI was to take the idea of international

security their complete and main priority. This strategy highlighted that the "key aspects of cyberspace – such as the difficulty of attributing an attack to its perpetrators or sponsors, and the dual-use nature of the technology – are seen...as inherently destabilizing" (Department of State International Cyberspace Policy Strategy 3). President Obama stressed that any possible foreign or domestic cyberattack would be devastating and that cybersecurity is a "matter of national security". It also mentioned the importance of banding together with other nations to protect and secure cyberspace so that everyone can use it equally.

On February 9 of 2016, President Obama released the Cybersecurity National Action Plan (CNAP), in order to make his strategy become a reality. The CNAP reiterated everything in the Obama Administration's cyberspace policy and then some, including the creation of a Commission on Enhancing National Cybersecurity. They would attempt to change the "way individuals and organizations perceive and use technology and approach cybersecurity as consumers and providers in the digital economy" ("Executive Order"). I believe that this stance made the United States a chief enforcer of cyber diplomacy and projected a very strong leadership role in the world.

Why is this Important?:

The modern economy is based on a global market that heavily relies on cyberspace and technology. According to the World Economic Forum, "Eighty per cent of the value of Fortune 500 companies now consists of intellectual property (IP) and other intangibles". Most of the world has their assets under intellectual property, which, unfortunately, is under constant attack from hackers. Specifically, one of the most recent cyberattacks was made by Russian and

Chinese hackers and "caused outages on popular websites from the U.S. east coast to Europe and Asia on October 21" (RFE/RL). These hackers did nothing particular to the websites nor their customers, but instead showed the possible threat could possibly pose towards the modern way of living. They also described several other companies and countries that they had supposedly hacked. In addition, NATO diplomats have reported that the hacking of the "alliance's network and facilities have skyrocketed by 60 percent over [2016]" (Sharkov). With these types of claims, it is irresponsible for America to ignore the threat of cyberattacks.

In recent years, there have been many cyberattacks from small to large scale on companies to people all over the world. In 2015, "companies saw an average of 160 successful cyber attacks per week, more than three times the 2010 average of 50 per week" (Walters), and it has only been increasing since then. The protection of cyberspace is not solely important to the United States, but to every country in the world. Under the Obama administration, it was stressed that there is a need for some type of "global security". It was then that the CCI, "in partnership with the Department of Justice and the Department of Homeland Security, [began leading] a campaign against transnational cybercrime" (Department of State International Cyberspace Policy Strategy 4-5). While the United States has policy towards cyber diplomacy has not gotten very far, we have been progressing at a faster pace than most nations.

Thus, other countries have followed suit in the United States' campaign, including many European countries. For example, the British Parliament approved an article called the Global Data Protection Regulation (GDPR) on April 14, 2016. This regulation would force "organizations proactive about their security at a boardroom level and prevent data breaches of

EU nationals from occurring" (Skroupa). With other countries following the United States' lead, it is impossible to back out of a cyber diplomacy policy.

Why Should We Care?:

The idea of having some type of regulation on cyberspace has been floating around the world for several decades. Yet, in past couple months, the Trump Administration has opened to the idea of destroying CCI and folding it within another larger department under the State Department. This is a complete change from the previous President's in-depth policy on cyberspace. Under President Trump, the White House is consistently seen as promoting the "marginalization of cyber issues in foreign policy" (Fidler) and belittling foreign diplomacies. The Trump Administration is more focused on it's 'America First' policy, and would chose to focus more on domestic policies. This is completely contradictory of the rest of the world which is constantly moving into a more digitally interconnected world.

The way this new administration has pushed off the Russian interference of the presidential election has confused many people, including, other politicians and the United States' allies. The 2016 G20 was one of the most anticipated meetings as it was the first time President Trump was on the international stage. In a press conference after the G20, President Trump stated that the interference during the 2016 presidential election "'very well could [have been] Russia but [he thinks] it could very well have been other countries'" (Chillizza). This went completely against what Rex Tillerson, the Secretary of State, told the media what happened during the meeting, as he emphasized that President Trump pushed hard on Vladimir Putin on

the meddling scandal. The complete apathetic attitude towards Russia from the President shows that the United States does not care if another country becomes involved in our elections.

A discord between the White House and the President should be a definite concern for the public. The President is suppose to reflect the opinions of the people, not his own beliefs ideology. Having the leader of the free world believing that the Russian hacking was only a possibility, is a weakness in the eyes of the rest of the world. As he completely disregarded the country's own intel from the FBI, President Trump has shown that he has no trust in the government his supposedly runs. This projects and unstable view of the United States to other nations.

Conclusion:

The possibility of a rival country attempting to interfere with the electoral process digitally is no longer a theory - it's a reality. In order to stay a world leader, the United States needs to keep up with the times. Cyber diplomacy needs to be an important issue to the government and the citizens. Our lives run on the internet. One major attack could wipe out the entire world's livelihood. It is the United States' duty to ensure that the pursuit of cyber diplomacy is continued.

Works Cited

Cillizza, Chris. "Trump Totally Changed His Tune on Russian Hacking Today. Why?" *CNN*, Cable News Network, 7 July 2017, www.cnn.com/2017/07/07/politics/trump-putin-russia-meddling/index.html.

Clinton, Larry , President and Chief Executive Officer, Internet Security Alli. "5 Economic Principles of Cyber Security." *World Economic Forum*, www.weforum.org/agenda/2015/02/5-economic-principles-of-cyber-security/.

DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY, Public Law 114-113, Division N, Title IV § 402 (2016). Print.

"Executive Order -- Commission on Enhancing National Cybersecurity." *National Archives and Records Administration*, National Archives and Records Administration, obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

Fidler, David P. "U.S. Cyber Diplomacy Requires More than an Office ." *Council on Foreign Relations*, Council on Foreign Relations, 26 July 2017, www.cfr.org/blog/us-cyber-diplomacy-requires-more-office.

"Office of the Coordinator for Cyber Issues." *U.S. Department of State*, U.S. Department of State, www.state.gov/s/cyberissues/index.htm.

"Presidential Proclamation -- National Cybersecurity Awareness Month, 2016." *National Archives and Records Administration*, National Archives and Records Administration, obamawhitehouse.archives.gov/the-press-office/2016/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2016

RFE/RL. "Hacking Group From Russia, China Claims Credit For Massive Cyberattack." *RadioFreeEurope/RadioLiberty*, RadioFreeEurope/RadioLiberty, 22 Oct. 2016, www.rferl.org/a/hacking-group-new-world-hacking-russia-china-claims-credit-twitter-massive-cyberattack-dyn-/28068649.html.

Sharkov, Damien. "NATO Reports Huge Surge in Cyber Attacks in 2016." *Newsweek*, 24 Jan. 2017, www.newsweek.com/nato-reports-huge-surge-cyber-attacks-2016-544554.

Skroupa, Christopher P. "Cyber Security Regulation -- The Move Towards Board Involvement." *Forbes*, Forbes Magazine, 31 Aug. 2017,www.forbes.com/sites/christopherskroupa/2017/08/31/cyber-security-regulation-the-move-towards-board-involvement/#34bfe68b4046.

Walters, Riley. “Cyber Attacks on U.S. Companies Since November 2014.” *The Heritage Foundation*, The Heritage Foundation, 18 Nov. 2015, www.heritage.org/cybersecurity/report /cyber-attacks-us-companies-november-2014.