Submitted 13 April 2020

Foreign Interference Background Report

By Abby Williams

As a platform on which the course of international politics unfolds, the internet poses a myriad of modern threats to democracy, such as hacking, disinformation, and the use of social media as a means of manipulating the public. The most notable example of this took place in 2016, when the United States presidential election was targeted by Russian operatives (Helderman & Zapotosky 2019). As the 2020 presidential election approaches, foreign interference has already begun, and Russia is no longer the only country at the source (Tucker 2019). China, Iran and other foreign adversaries are being identified as threats, but their attacks are not limited to the United States alone, as an alarming number of democratic nations have been infiltrated worldwide, including Australia (International Cyber Policy Centre 2019).

By analysing the strategies behind Russia's cyberattacks in 2016, this background report will offer an understanding of the threats posed to the US 2020 presidential election, as well as other nations which are susceptible to foreign interference. As a widespread issue with global ramifications, it is necessary that both governments and individuals understand the nature of cyber threats and their potentially damaging role in politics.

How cybercrime and disinformation disrupted the 2016 United States presidential election

The internet has become a fundamental component in political and social matters, as well as an instrument in the exercise of power (Franklin 2014, p. 180). It plays an integral role in the lives of its 4.5 billion users (Internet Live Stats n.d.), and supports equity by enabling citizens to participate in the matters which affect them (International Cyber Policy Centre 2019). However, as the world's reliance on the internet increases, so too do the threats to its users. The growing prevalence of cybercrime paired with the spread of disinformation on social media renders users vulnerable to cyberattacks and manipulation (International Cyber Policy Centre 2019). When users' rights to privacy and information are undermined by such attacks, so too is democracy.

While hacking is a form of computer trespassing which involves gaining unauthorised access into a computer system (McQuade 2009, p. 87), ‘internet trolling’ involves deceptive, destructive or disruptive behaviour in an online social environment (Buckels et al., cited in Dynel 2016). Cyberattacks can be launched by both large, state-sponsored hacking groups, and non-state hackers (Sigholm 2013). Similarly, discord and confusion can be traced back to individual internet trolls, as well as large, organised ‘armies’ known as ‘troll factories’ (Goldman et al. 2020). By breaching the rights of internet users and stoking social unrest, hackers and trolls are capable of generating not only chaos, but disinformation and political interference.

The politically disruptive power of hacking and trolling was exemplified in 2016, when Russian operatives interfered in the US presidential election by planting false news stories and fuelling controversial debates amongst voters (Helderman & Zapotosky 2019, p. 24). An investigation carried out by Special Counsel Robert S. Mueller III exposed the methods of a Russian troll factory, known as the *Internet Research Agency*, who interfered with the election by posing as US citizens on social media and posting derogatory content regarding presidential candidates (Department of Justice 2018). Mueller’s findings confirmed that these Russian operatives ultimately influenced the course of politics (Helderman & Zapotosky 2019, p. 24). Now, as the 2020 US presidential election approaches, it’s happening again.

Why the US is bracing itself against foreign interference again, and how the threat has evolved

In February this year, US intelligence officials warned that Russia was actively interfering with the 2020 presidential election process (Goldman et al. 2020). By repeating the tactics used to misinform and divide the public in 2016, Russian operatives are again supporting President Donald Trump’s campaign (Goldman et al. 2020). Having learned from the situation in 2016, the American government is implementing additional security measures to increase its defence against foreign disruption in the democratic process (National Security Agency 2019). Although the government’s approach to cybersecurity has evolved, so has Russia’s approach to infiltrating the system, as well as their ability to do so undetected (Rosenberg, Perlroth & Sanger 2020). However, Russia is no longer the only source of interference, as China and Iran have been identified as threats to the presidential campaign (National Security Agency 2019).

By studying the divisive methods used by Russia in 2016, China and Iran are developing strategies by which they are disrupting the electoral process (Tucker 2019). In October 2019, a hacking group believed to be of Iranian origin attempted to break into President Donald Trump's re-election campaign (Bing & Satter 2019), as well as email accounts belonging to US government officials and journalists covering global politics (Burt 2019). Like Russia, Iran is using social media to spread disinformation and influence public opinion (Sebenius 2019). China, however, has advocated for policies using conventional media outlets (Sebenius 2019), and has utilised its cyber capabilities as a means of intellectual property theft, espionage (Tucker 2019), and furthering its emergence as a global economic superpower (Silver, Devlin & Huang 2019). Regardless of the methods, the underlying objective is to manipulate voters and weaken the foundations of American democracy (National Security Agency 2019).

While Russia, China and Iran pose the most significant threats to the 2020 US presidential election, foreign disruption is far from limited to these three nations. America's role as a global superpower means that the electoral outcome will have an overwhelming impact throughout the world (West 2019). As US policies affect economic development opportunities globally, countries which are most reliant on this outcome are also the most likely to attempt to influence it (West 2019). Therefore, North Korea and Saudi Arabia have also been classified as potential threats (West 2019); however, due to America's global influence and the insecure nature of the internet, it would be virtually impossible to quantify the number of foreign adversaries who pose a risk.

How the United States is defending democracy, and why governments and citizens worldwide should be paying attention

As the internet evolves, creating an ideal environment for cybercrime and political disruption, America is restructuring its approach to defence against foreign interference.

The Federal Bureau of Intelligence (FBI) is investigating foreign influence operations, and is working toward wider recognition of the threat and the development of strategies against it (Federal Bureau of Intelligence n.d.). The federal government is further protecting the democratic process by securing the nation's election infrastructure and sharing threat intelligence (National Security Agency 2019). Microsoft is monitoring hacking groups and disclosing its findings to the public (Burt 2019). Facebook and Twitter are suppressing hackers by removing not only fake accounts, but entire foreign propaganda operations (Greene, Romm & Nakashima 2019).

The US 2020 presidential election is currently at the forefront of international politics; however, cybercrime and foreign disruption have no geographical limitations, rendering countless countries worldwide vulnerable to political disruption (International Cyber Policy Centre 2019). A study carried out by the Australian Strategic Policy Institute (ASPI) identified foreign interference in the electoral processes of 20 democratic nations (including 'flawed' democracies) between November 2016 and April 2019 (International Cyber Policy Centre 2019). This list of countries includes Australia, where Chinese operatives allegedly hacked major political parties, and federal Parliament's computer systems (Wroe 2019). Unlike what happened in the US, many of these interference attempts did not play out on a global stage. However, it is vital that governments understand the issue in its entirety so that they too can strengthen their defences against disruption.

While governments worldwide are facing the challenges posed by the nature of the internet, it is important not to underestimate the resilience of an informed public (National Security Agency 2019). The magnitude of the electoral disruption in America has created a model on which other countries can develop strategies to oppose foreign influence (International Cyber Policy Centre 2019). However, while nations restructure their approaches to cybersecurity, individuals are also responsible for understanding the threats to their rights as citizens, and the divisive tactics used by foreign adversaries (National Security Agency 2019). As the internet evolves, so too should our awareness of its potential for disinformation and voter manipulation (Kaplan 2019).

Conclusion

Although the internet enables users to engage in political processes, its insecure nature renders it a platform for cyberattacks, voter manipulation, and foreign interference (International Cyber Policy Centre 2019). Its politically destructive potential was fully recognised in 2016, as Russian operatives undermined the US presidential election (Department of Justice 2018). In 2020, as the threats to the upcoming election grow to include countries such as China and Iran (Tucker 2019), America is strengthening its defences (National Security Agency 2019), but governments worldwide should also be developing strategies to defend their nations and the rights of their citizens (International Cyber Policy Centre 2019). A vigilant understanding of the capabilities of hackers and trolls can help internet users to recognise and suppress disinformation and disruption (Kaplan 2019). Where the dangers of the internet threaten to erode the foundations of democracy, we as informed citizens have the ability strengthen it.

References

Bing, C & Satter, R 2019, ‘Trump re-election campaign targeted by Iran-linked hackers: sources’, *Reuters*, 5 October. Available from: https://www.reuters.com/. [19 March 2020].

Burt, T 2019, ‘Recent cyberattacks require us all to be vigilant’, *Microsoft On the Issues*, blog post, 4 October. Available from: https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/. [19 March 2020].

Department of Justice 2018, *Internet Research Agency Indictment,* United States Government. Available from: https://www.justice.gov/file/1035477/download. [5 April 2020].

Dynel, M 2016, ‘“Trolling is not stupid”: Internet trolling as the art of deception serving entertainment’, *Intercultural Pragmatics*, vol. 13, no. 3, pp. 353-381. Available from: De Gruyter. [5 April 2020].

Federal Bureau of Intelligence n.d., *Combating Foreign Influence*. Available from: https://www.fbi.gov/investigate/counterintelligence/foreign-influence. [9 April 2020].

Franklin, MI 2014, ‘How does the way we use the internet make a difference?’ in J Edkins & M Zehfuss, (eds), *Global Politics: a New Introduction*, 2nd edn, pp. 176-199. Routledge, New York.

Goldman, A, Barnes, JE, Haberman, M & Fandos, N 2020, ‘Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump’, *The New York Times*, 20 February. Available from: https://www.nytimes.com/. [19 March 2020].

Greene, J, Romm, T & Nakashima, E 2019, ‘Iranians tried to hack US presidential campaign in effort that targeted hundreds, Microsoft says’, *The Washington Post*, 5 October. Available from: https://www.washingtonpost.com/. [9 April 2020].

Helderman, S & Zapotosky, M 2019, *The Mueller Report,* Simon & Schuster, London.

International Cyber Policy Centre 2019, *Hacking Democracies: Cataloguing cyber-enabled attacks on elections*, Australian Strategic Policy Institute. Available from: https://www.aspi.org.au/report/hacking-democracies. [9 April 2020].

Internet Live Stats n.d., *Internet Users in the World*. Available from: https://www.internetlivestats.com/watch/internet-users/. [5 April 2020].

Kaplan, L 2019, '4 steps to stop the spread of disinformation online', *Brookings Institution,* blog post, 23 July. Available from: https://www.brookings.edu/. [9 April 2020].

McQuade, SC (ed) 2009, Encyclopedia of Cybercrime, Greenwood Press, Westport.

National Security Agency 2019, *Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections*. Available from: https://www.nsa.gov/news-features/press-room/Article/2009338/joint-statement-from-doj-dod-dhs-dni-fbi-nsa-and-cisa-on-ensuring-security-of-2/. [7 April 2020].

Rosenberg, M, Perlroth, N & Sanger, DE 2020, ''Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020', *The New York Times*, 10 January. Available from: https://www.nytimes.com/. [6 April 2020].

Sebenius, A 2019, 'US Sees Russia, China, Iran Trying to Influence 2020 Elections', *Bloomberg*, 25 June. Available from: https://www.bloomberg.com/. [21 March 2020].

Sigholm, J 2013, 'Non-State Actors in Cyberspace Operations', *Journal of Military Studies,* vol. 4, no. 1, pp. 1-37. Available from: ResearchGate. [10 April 2020].

Silver, L, Devlin, K & Huang, C 2019, *China's Economic Growth Mostly Welcomed in Emerging Markets, but Neighbors Wary of Its Influence*. Available from: https://www.pewresearch.org/global/2019/12/05/chinas-economic-growth-mostly-welcomed-in-emerging-markets-but-neighbors-wary-of-its-influence/. [8 April 2020].

Tucker, E 2019, 'Threat to US elections in 2020 is not limited to Russia', *Associated Press*, 31 October. Available from: https://apnews.com/. [19 March 2020].

West, DM 2019, 'Foreign campaign intervention may go way beyond Russia to China, Iran, North Korea, and Saudi Arabia', *Brookings Institution,* blog post, 9 August. Available from: https://www.brookings.edu/. [9 April 2020].

Wroe, D 2019, 'China key suspect in pre-election hack against major parties', *The Sydney Morning Herald*, 18 February. Available from: https://www.smh.com.au/. [9 April 2020].