doi:10.1017/aju.2020.87

SYMPOSIUM ON THE BIDEN ADMINISTRATION AND THE INTERNATIONAL LEGAL ORDER

A ROADMAP FOR FIGHTING ELECTION INTERFERENCE

*Jens David Ohlin**

If we have learned anything since the 2016 election, it is that foreign election interference is not just a strategic tool used by Russia. Many countries are now using social media disinformation as statecraft to attack democracies. With a relatively small investment of personnel and financial resources, a foreign power can use social media and other online tools to heighten divisions in the electorate, spread disinformation and conspiracy theories, and undermine confidence in the electoral system specifically and democratic institutions generally. The Biden administration should use the moral, political, and legal authorities of the Executive Branch to protect the United States from foreign election interference. In parallel, it should work cooperatively with allies to combat election interference using multilateral initiatives.

What is Election Interference and Why Does it Matter?

The term election interference is used to describe a variety of measures, both foreign and domestic, that impact the conduct of elections. This essay's focus is on a particular flavor of election interference: the use of cyber-tools by governments, or non-state actors working in close collaboration with them, to influence elections. In that regard, I am particularly concerned with two examples of this phenomenon: the hacking and public release of private information, and social media activity authored by foreign troll farms. In each instance, the activity is usually pursued covertly, in the sense that the foreign nature of the intrusion is not readily acknowledged by the actor behind the operation.

Take just one notable example: During the 2016 election, Russian government agents hacked email accounts associated with Democratic campaign officials, including John Podesta. These emails were then released to the public prior to the 2016 presidential election. At first, the Russian intelligence service (GRU) created a fake organization called "DC Leaks" to disclose the information online through Twitter, a fake Facebook page, and emails sent to reporters. The choice of name for the organization was deliberate—it was designed to create the appearance that the emails were hacked and released by a DC political insider, rather than by a foreign state.

As a second example, the Internet Research Agency (IRA) operated a troll farm in St. Petersburg to create a large number of social media posts for Twitter, Facebook, and Instagram.[1] These posts introduced new topics into the political landscape and increased the audience for existing posts by strategically sharing them, either individually or through bot accounts. For instance, some messages suggested that the electoral process was rigged and that African Americans should boycott the election. The strategic goal of the effort was to heighten ideological and

* *Interim Dean and Professor of Law, Cornell Law School, Ithaca, New York, United States.*

[1] *See* Renee DiResta et al., The Tactics & Tropes of the Internet Research Agency (Oct. 2019).

© Jens David Ohlin 2021. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/aju.2020.87 Published online by Cambridge University Press

political divisions, sow distrust in the electoral system, undermine confidence in democracy, and help elect Donald Trump president of the United States.[2] The social media posts authored by the IRA troll farm were authored covertly, in the sense that the foreign nature of these accounts was not readily apparent to those who read the tweets, and indeed the content was designed to appear American in origin.

Discussions about foreign election interference often get bogged down over questions of significance. Did Russian intervention in the 2016 election actually change the result? Two observations are important here. First, the margin of victory in the 2016 election was exceedingly small, with about 80,000 votes over three Rust Belt states making the difference between a Clinton win and a Trump win. Consequently, even if Russian interference only made a small difference at the margins, this could have had a decisive impact.[3] Second, even assuming that the interference made no difference to the outcome of the election, the nation should take the threat of foreign election interference seriously. The danger posed by a particular threat is measured not by the actual damage caused but rather by the potential disruption it represents.

Before articulating the steps that the Biden administration should take to stop foreign election interference, it is necessary to briefly explain why the behavior violates international law and does not constitute legally protected international statecraft. There are three potential frameworks for evaluating the legality of election interference: cyberwar, sovereignty/non-intervention, and self-determination.

Politicians often describe foreign election interference as a cyber-attack against the nation, or as an act of war. While there is still some uncertainty over how to apply jus ad bellum and jus in bello principles to the cyber domain, the prevailing (and in my view correct) view is that a cyber-attack can only rise to the level of a jus ad bellum violation if it triggers some destructive consequence, i.e., it destroys a physical installation or injures human beings. (There is some dispute over whether a cyber-attack that merely "disables" a computer system or other infrastructure would qualify.) While modern methods of social media disinformation are troubling, they are not troubling in the right way for purposes of jus ad bellum—they do not produce physical destruction, nor do they disable computerized infrastructure.

The second paradigm—sovereignty and the principle of non-intervention—is initially far more promising. This not only accords with a common-sense view (that Russia infringed U.S. sovereignty by interfering in elections) but also dovetails with a core doctrine of public international law, i.e., that states should not interfere with the *domaine réservé* of other states. Unfortunately, there are doctrinal obstacles here, including the requirement announced by the International Court of Justice in *Nicaragua v. United States* that an intervention must be coercive in order to qualify as unlawful. It is hard to identify how modern disinformation campaigns are coercive. They are best described as corrosive, not coercive.

There are two potential routes that an answer to this skeptical challenge might take. The first is to shift from non-intervention to a so-called "stand alone" concept of sovereignty, outside of the narrow doctrine of non-intervention. The second is to shift to an entirely new paradigm, such as self-determination. As I have argued elsewhere, the collective right of self-determination protects the right of a people to select their own destiny, which in a democratic polity is expressed through the institution of elections.[4] This collective right provides a conceptual justification for boundary regulations that define the outer limits of the polity: rules on who may vote in an election, including those defining citizenship and residency; rules on who may participate in elections through financial contributions; and transparency regulations such as the Foreign Agents Registration Act, which requires agents of foreign state actors to identify themselves when they engage in lobbying and other political efforts. While there is

[2] *See* Office of the Director of National Intelligence, Intelligence Community Assessment, Assessing Russian Activities and Intentions in Recent US Elections, ICA 2017-01D, at ii (Jan. 6, 2017).

[3] *See* Kathleen Hall Jamieson, Cyberwar: How Russian Hackers and Trolls Helped Elect a President (2018).

[4] Jens David Ohlin, Election Interference: International Law and the Future of Democracy (2020).

https://doi.org/10.1017/aju.2020.87 Published online by Cambridge University Press

nothing inherently wrong with foreign states or foreign officials expressing their views about U.S. electoral politics, including support for one political candidate over another, this support violates the collective right of self-determination when it is done systematically, surreptitiously, and covertly.

How to Stop Election Interference

In order to stop foreign election interference, the Biden administration ought to take the following unliteral and multilateral actions:

(1) Make Unambiguous Public Statements that Foreign Election Interference Violates International Law. While the federal government (with the possible exception of Donald Trump) has been relatively clear that foreign election interference poses a threat to the political integrity of the United States, the government has not been clear on whether such actions violate international law. This hesitation goes back to the Obama administration, which specifically declined to call the Russian interference a violation of international law, preferring instead to describe it as a violation of acceptable norms of international behavior.[5] It is unclear why exactly the Obama administration was so cautious in its language. Whether it wanted to preserve its own authority to engage in similar actions, or it did not want to commit itself to a particular response, the hesitation endured throughout the Trump administration.

The Biden administration must work cooperatively with other democratic states to clearly articulate that election interference violates customary international law. An important step in the creation of customary international law is state action and opinio juris, both of which can be advanced through official statements by governments. To foster the development of customary norms in this area, the Biden administration could work multilaterally to issue a joint statement with other nations, or even work collectively to develop soft-law mechanisms.[6] For example, New Zealand recently issued a formal statement declaring that a cyber-activity is illegal when it interferes with a state's right to freely choose its "political, economic, social and cultural system" or "deprives a significant part of the electorate of the ability to vote."[7]

(2) Impose Economic Sanctions on Foreign Actors that Engage in Election Interference. The Biden administration needs to vigorously punish foreign actors who engage in election interference. In particular, economic sanctions should be targeted against individuals who are closely related to the election interference, either because they are engaged in the activity, have a funding relationship to it, or enjoy illicit business relationships with the foreign leader responsible for instigating the election interference. For maximum impact, multilateral sanctions through the Security Council would be preferable, but Russian and Chinese vetoes make that unlikely. However, parallel sanctions coordinated with the European Union and other states could be pursued.

Although the United States imposed unilateral sanctions against individuals in Russia suspected of involvement in foreign election interference, the Trump administration's confusing rhetoric surrounding the issue blunted the expressive impact of these sanctions. Foreign actors may have legitimately questioned either the U.S. government's resolve in stopping election interference or questioned the degree of unity in the federal government on this issue. To take just one famous example, incoming National Security Advisor Michael Flynn told the Russian Ambassador prior to Trump's inauguration that Trump planned to roll back the sanctions. The Biden administration should speak with one voice in both condemning election interference and promising a consistent practice of economic sanctions when it occurs.

[5] The White House, Office of the Press Secretary, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016) (describing "established international norms of behavior").

[6] For an example of one such statement issued by individual scholars, see Dapo Akande et al., *Oxford Statement on International Law Protections Against Foreign Electoral Interference through Digital Means*, Just Security (Oct. 28, 2020).

[7] *See* New Zealand Office of Foreign Affairs, The Application of International Law to State Activity in Cyberspace (Dec. 1, 2020).

https://doi.org/10.1017/aju.2020.87 Published online by Cambridge University Press

(3) Clarify Federal Authority to Stop Election Interference. The Biden administration, with Congress, needs to move swiftly to alter the federal bureaucracy to resolve any ambiguity over which federal agencies have the authority to combat foreign election interference. Currently, a variety of agencies have authority over different aspects of election security. For example, the Cybersecurity and Infrastructure Security Agency, created in 2018, is doing important work on protecting election infrastructure, but its work relates more to the process of electioneering and is less related to foreign interference that impacts the substance of democratic deliberation. The National Security Agency, the Federal Bureau of Investigation's Counter-intelligence Division, and the Central Intelligence Agency investigate foreign interventions such as troll farm activity, but any actions that they take in response are usually classified and confidential. Finally, the Justice Department may engage in non-classified responses, such as the filing of indictments, but those public actions are limited to situations where there is a violation of federal criminal law.

The result of this patchwork of agency jurisdictions is that the most important form of foreign election interference gets short shrift: foreign-funded social media disinformation campaigns that focus on political substance rather than political process. To be sure, it is hazardous to have a federal government agency policing content that is overtly political in nature. But it is worthwhile to remember that foreign election interference can be defined (and fought) in a politically neutral way, based solely on its foreign source and regardless of which candidate is helped or harmed by the intervention.

(4) Encourage the Justice Department to Issue More Indictments. The Justice Department should continue, and indeed augment, its practice of filing criminal indictments against individuals or corporations involved in foreign election interference. This prosecutorial practice originated with the team working for Special Counsel Robert Mueller,[8] but hopefully the practice will survive his departure and remain a central policy of the Justice Department under a new Attorney General. Many have wondered why such indictments are advisable or useful, especially since the named individuals or corporate entities are located outside of the territory of the United States, are not in the habit of traveling here, and hence will never be brought to justice. While true, this misses the point about these innovative indictments. While indictments are usually designed as a prelude to trial, possible conviction, and punishment, criminal indictments in the national security context have other benefits outside of the traditional purview of criminal justice.

First, indictments provide timely information to the public about foreign election interference that the public otherwise may not receive. Much of the information about foreign election interference is collected and maintained by intelligence agencies, such as the National Security Agency or the Central Intelligence Agency, that do not have a tradition or culture of disclosing information to the public. Indeed, the culture of these agencies is to protect classified information, rather than to engage in strategic disclosures to the American public. Consequently, this role falls to other federal agencies. The Justice Department's practice of indicting individuals responsible for election interference has the practical consequence of informing the public about the foreign involvement. The Justice Department adopted a new policy in 2018 designed to encourage the disclosure of foreign influence operations, but due perhaps to an entrenched culture among counterintelligence agents, the policy has had minimal impact.[9] Until that changes, indictments provide a ready avenue for public disclosure.

Second, criminal indictments provide a valuable service by attributing the source of any cyber-attacks associated with the foreign election interference. Attribution to a foreign state is an important preliminary step in holding foreign states responsible for misbehavior in this context.[10] It has been noted that attribution in the cyber context

[8] United States v. Internet Rsch. Agency LLC et al., Indictment, 18-CR-32 (D.D.C. Feb. 16, 2018).

[9] Justice Manual § 9-90.730 - Disclosure of Foreign Influence Operations.

[10] Chimène I. Keitner, *Attribution by Indictment*, 113 AJIL UNBOUND 207 (2019).

https://doi.org/10.1017/aju.2020.87 Published online by Cambridge University Press

is difficult, though nothing in international law prohibits attribution by inference to the best possible explanation. Criminal indictments are official accusatory documents from the government that can address both internal and external audiences. The internal audience in this context is the U.S. public and the U.S. judiciary, whereas the external audience is the community of nations that reads the indictment and learns that the U.S. government believes that a particular foreign actor is responsible for the misbehavior.

(5) Criminalize Solicitation of Foreign Interference. Congress should pass a federal statute explicitly criminalizing the solicitation of foreign involvement in a U.S. election. During the impeachment of President Trump, a central allegation was that he solicited foreign involvement during his phone call with Ukrainian President Volodymyr Zelensky. At the time, there was some uncertainty over whether this conduct violated federal criminal law, apart from whether the conduct was impeachable. The phone call could be analyzed under existing federal statutes and regulations on a variety of topics, including campaign finance, conspiracy, and extortion. Nonetheless, none of these authorities capture the distinctive harm associated with the phone call—the solicitation of foreign involvement in a domestic election. For the removal of all doubt, it would be beneficial for Congress to clarify that such solicitations violate federal criminal law. Doing so would not necessarily concede that the phone call was proper or lawful, it would simply clarify a situation that was admittedly unclear under existing law.

(6) Encourage Social Media Firms to Label Foreign Conduct. Finally, social media firms should take more expansive steps to label political content with a foreign origin. Social media firms such as Twitter and Facebook already identify and shut down accounts linked to state-run troll farms engaged in election interference. The social media firms also flag as "disputed" posts from domestic accounts that spread disinformation. These actions are laudable and should continue. But a labeling regime for foreign posts would sweep far broader than current efforts designed to shut down state-run troll farm accounts and could be applied in a content-neutral way. One objection to a broader labeling regime is that masking technology makes it easy for account holders to hide their true origin, which would prevent social media companies from identifying foreign account holders. But there might be creative solutions to these technological barriers; accounts could be labeled as presumptively foreign until users take affirmative steps to conclusively demonstrate their domestic status.

Although First Amendment concerns loom large in the context of social media regulation, several factors would insulate such labeling practices from constitutional concern. First, these actions should be taken voluntarily by social media platforms, rather than mandated by the government. Second, the regime would involve labeling rather than censorship. There is less constitutional scrutiny when a social media platform imposes its own speech on top of the user's speech—in the same way that Twitter adorns, or fails to adorn, some accounts with blue checkmarks. Third, a labeling regime would only target foreign actors located on foreign territory, who do not have a First Amendment right to participate in U.S. elections anyway.

Conclusion

The 2020 presidential election focused the national conversation around domestic disinformation. Why should we care about foreign election interference when national leaders, including the president, distribute discredited conspiracy theories over social media? Foreign interference constitutes a distinctive harm not found in domestically generated disinformation because *foreign* interference risks undermining the foundation of democracy, which is to ensure that elections fulfill the collective right of self-determination. The six recommendations outlined above are necessary to protect that collective right.

https://doi.org/10.1017/aju.2020.87 Published online by Cambridge University Press