



**Malcolm Wallop Civic Engagement Program
K-12 Curriculum Project**

History of Elections Hacking – Teacher Resource Guide

Laura Baker, Board President
CyberWyoming Alliance

Targeted Grades: Middle School (6-8)/High School (9-12)

Wyoming Social Studies Standards Lesson Aligns With:

- 8th grade standards: SS8.1.1, SS8.1.2, SS8.4.1, SS8.4.2 and SS8.4.3.
- High school standards: SS12.1.1, SS12.1.2, SS12.4.1, SS12.4.2 and SS12.4.3.

Presentation Summary:

Cybersecurity is a growing concern among governments, businesses, and citizens in the United States and around the world. One aspect of this, foreign election hacking, has become a growing challenge to modern democracies, including the United States. By definition, election hacking (or more broadly election tampering) is the attempt by governments (and non-government groups) to covertly or overtly influence the elections of another country. This presentation looks at the allegations of recent election hacking in the United States, its origins, and raises questions about the implications this has for our democracy. The presentation traces the origins of Russian hacking to the 2014 Sochi Winter Olympics in Russia and presents a number of questions for your students to ponder about the implications this has for democratic elections and the future of American democracy. As you review the presentation in class, you can ask students about what they already *knew* and what they learned from this video to set up a discussion of broader implications for hacking and cyberspace for election security and beyond.

Suggested Discussion Questions:

1. Do you think election hacking should be taken more seriously today? Why or why not?
2. Should campaigns be responsible for their own cybersecurity? Why or why not?
 - a. Possible class activity: Your students can learn more about the cybersecurity training that is available and techniques available to counter the influence of hacking.
3. How has cyberspace shaped the relationship between countries? How has cyberspace blurred the line between peace and war? What did Russia gain or what does any country potentially gain from these actions?
 - a. Possible class activity: Students could look at the cyberwarfare doctrines of other countries and look at how this issue is viewed among American allies. (John Carlin in *Dawn of the Code War* references 41 countries that have cyberwarfare doctrines and 17 countries that have offensive capabilities in cyberspace.) Students could do a Google search for an article to bring into class as the basis of a discussion that puts the American situation into a broader perspective.
4. What do you think our government agencies need to do to adapt to the world of cyberspace? How can/should national/state/local governments respond? What has been done in Wyoming and locally?

- a. Possible class activity: Students could interview the local county clerk or someone from the Wyoming Secretary of State's Office to ask about their concerns and election security measures.
- b. Possible class activity: Look into how your school or school district is responding to cyber hacking and student security. Has this become an issue of concern? Identify a point person from class(es) to gather information.
5. How widespread is the concern among US government agencies about the threat of cyber hacking?
 - a. Possible class activity: Students can look into the different cyber strategies in the US originating from different government agencies such as the White House, the Department of Homeland Security, the FBI, the Department of Commerce, US Cyber Command, the Department of Defense, the Department of Justice, and the Cyberspace Solarium Commission.
6. What in cyberspace could impact your life? What are the positives and negatives?
7. What precautions do you take as an individual to secure your important information?
8. If this is used in an American or world history class, recent allegations of Russian hacking are not the first illustration of election hacking or election interference. Current circumstances could be used as a lens to discussing election tampering during the Cold War on the part of the United States or Soviet Union.

Sources for Additional Information on the Topic:

Carlin, John, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (New York: Hachette Book Group, 2018)

- Videos featuring John Carlin talking about his book, *Dawn of the Code War*, and telling stories:
<https://www.c-span.org/video/?455540-1/dawn-code-war>
<https://www.youtube.com/watch?v=sYCQRy2Xgo>
 Specifically about China: <https://www.youtube.com/watch?v=OBavR7c7t4s>

Marks, Joseph. "Trumps Former Homeland Security Advisor Says Russia Remains Major Election Hacking Threat," *The Washington Post*, October 21, 2020,
<https://www.washingtonpost.com/politics/2020/10/21/cybersecurity-202-trumps-former-homeland-security-adviser-says-russia-remains-major-election-hacking-threat/>

US Department of Justice Links:

- <https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and>
- <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>
- <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>

Wyoming Secretary of State Office: <https://sos.wyo.gov/>

- Wyoming's Elections Code: <https://sos.wyo.gov/Forms/Publications/ElectionCode.pdf>
- Wyoming Internet Related Statutes: Wyoming Title 40 (consumer protection 40-12-501 through 40-12-902) <https://wyoleg.gov/statutes/compress/title40.pdf> and Wyoming Title 6 (criminal code 6-3-901 through 6-3-507 and 6-3-803) <https://wyoleg.gov/statutes/compress/title06.pdf>

World Anti-Doping Agency (WADA): <https://www.wada-ama.org/>

Contacting the Wallop Team: For information on how to schedule a chat-back "Ask Me Anything" session with Laura Baker or for more information on this or other modules contact the Wallop Program Team at wallop@uwyo.edu.