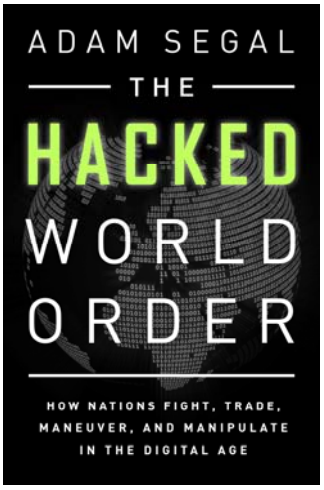
COUNCIL on FOREIGN RELATIONS

58 East 68th Street, New York, New York 10065
tel 212.434.9400 fax 212.434.9800 www.cfr.org



Teaching Notes
The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age

By **Adam Segal**
Maurice R. Greenberg Senior Fellow for China Studies and Director of the Digital and Cyberspace Policy Program, Council on Foreign Relations

PublicAffairs
February 2016
$26.99 paperback
320 pages
ISBN 978-1-610-39415-4

In *The Hacked World Order*, Adam Segal shows how governments use the web to wage war, spy on, coerce, and damage each other. While scholars, activists, and technologists initially heralded the Internet as a space outside of state control, governments have been quick to step into this new domain—both to control activity that happens within it and to adopt it as a new tool of state power.

The Hacked World Order analyzes the differing approaches that states have taken to control and weaponize the Internet. Israel is intent on derailing the Iranian nuclear weapons program. Russia uses proxies to launch disruptive cyberattacks on its neighbors. Brazil has plans to lay new fiber cables and develop satellite links so its Internet traffic no longer has to pass through Miami. China does not want to be dependent on the West for its technology needs. The United State pressures technology companies to provide "backdoors" and other methods to access encrypted data.

This book is suitable for undergraduate and graduate courses on international relations and U.S. foreign policy.

Discussion Questions

Courses on international relations

1. Two broad foreign policy approaches to the Internet have emerged: one advocates a free, open, global Internet and a multistakeholder model of global governance involving states and private actors, while the other supports limiting the flow of certain information online and a state-centric, multilateral model of governance. What motivates each of these approaches?

2. How revolutionary is cyberspace? In what ways have policymakers and academics struggled to apply traditional concepts in international relations to cyberspace?

3. What are the effects of cyber weapons on international stability? Is deterrence possible? Does the offense always have the advantage over the defense?

4. What are some of the challenges to Westphalian sovereignty—particularly state control over what goes on within their borders—presented by the Internet? How have states reacted to the loss of absolute power in cyberspace?

5. How does cyberwar differ from traditional warfare, if at all? What picture of cyberwar is presented in *The Hacked World Order*? Do you agree with the vision of cyberwar Segal outlines?

Courses on U.S. foreign policy

1. The United States government promotes a "global, open, secure, and resilient Internet." Why do U.S. policymakers see this as a matter of national interest?

2. What rules have U.S. policymakers identified for the use of force in cyberspace?

3. How has the Internet changed the way U.S. foreign policy officials interact with audiences at home and abroad? In what ways have they been proactive in responding to these changes, and in what ways have they fallen short?

4. United States officials have made a distinction between cyber-enabled espionage that steals political and military secrets and espionage that targets commercial secrets. Is this a meaningful distinction? Why have some foreign governments resisted recognizing this distinction?

5. How does the United States ensure that the pursuit of security in cyberspace does not undermine competing economic and foreign policy interests?

Essay Questions

Courses on international relations

1. What norms of state action in cyberspace have different governments promoted? What has caught on and what has not? What does this tell us about how international norms are formed?

2. If a criminal hacker in Russia uses a computer in France as part of an attack that temporarily shuts down a power plant in the United States, do any of these states have a responsibility to act? What types of responses would be justified?

Courses on U.S. foreign policy

1. Has the United States government been consistent in its efforts to realize a "global, open, secure, and resilient Internet?" If not, why? Is it possible to maintain each of these standards at once or will trade-offs be necessary?

2. How should the United States balance individual rights and government interests in cyberspace? Identify and explain a specific case where these rights and interests are in competition.

Further Projects

Policy Memo

The government of China has recently constructed a radar installation on a geographic feature in the South China Sea that is also claimed by U.S. regional partners. The Secretary of Defense has proposed conducting a military cyberattack to disable the radar installation in response. Write a one page memo for the President in which you analyze policy considerations related to such an action by the United States. These could include the proportionality of the response; potential for collateral damage; effectiveness in comparison to other potential responses; risk of miscalculation and escalation; and any potential Chinese reactions.

Op-Ed

Write an eight hundred word op-ed arguing for or against a national data localization policy (Chapter 6, "The Battle Over Data") from the perspective of a non-United States citizen.

Class Debate

Governments have been quick to adopt cyber means as a tool for intelligence gathering, attracted both by the large amounts of sensitive information stored and transmitted on computer networks as well as the difficulties of sure attribution of cyber intrusions. Have students read chapter five, "Everybody Spies," which examines cyber-enabled espionage. Organize a debate in which students argue for or against increasing the resources the United States government expends on cyber espionage. Conclude by leading a discussion on which side debated most persuasively, and why.

Supplementary Materials

"APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 19, 2013.

"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," The White House, May 2011.

"We Can Absolutely Not Allow the Internet to Become a Lost Territory of People's Minds," *PLA Daily*, May 12, 2015, translated by Rogier Creemers, *China Copyright and Media*, May 13, 2015.

David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment," *ISIS Reports*, December 22, 2010.

John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993): 141–165.

Ivanka Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme," *RUSI Journal* 158, no. 2 (April 2013): 48-56.

David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyberpower* (New York: Routledge, 2012).

Ron Deibert and Rafal Rohozinski, "Shadows in the Cloud: Investigating Cyber Espionage 2.0," Information Warfare Monitor, Shadowserver Foundation, April 6, 2010.

Laura Denardis, *The Global War for Internet Governance* (New Haven, CT: Yale University Press, 2015).

Dan Geer, "We Are All Intelligence Officers Now," YouTube video, RSA Conference, May 3, 2014.

Jennifer Granick, "The End of the Internet Dream," *Backchannel*, August 17, 2015.

Michael Joseph Gross, "World War 3.0," *Vanity Fair*, May 2012.

Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, (Vienna, VA: 2013).

Jason Healey, "The Five Futures of Cyber Conflict and Cooperation," *The Atlantic Council*, December 14, 2011.

Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, (New York: Simon & Schuster, 2016).

Robert K. Knake, *Internet Governance in an Age of Cyber Insecurity* (New York: Council on Foreign Relations Press, 2010).

Franklin Kramer, *Cyberpower and National Security*, (Lincoln, NE: Potomac Books, 2009).

James R. Langevin et al., "Securing Cyberspace for the 44th Presidency," CSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, December 2008.

Herbert S. Lin, "Arms Control in Cyberspace: Challenges and Opportunities," *World Politics Review*, March 6, 2012.

Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365-404.

Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Boston: The MIT Press, 2013).

Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series*, no. 1 (May 2014).

Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options (Washington: National Research Council, 2010).

Thomas Rid, *Cyber War Will Not Take Place*, (New York: Oxford University Press, 2013).

Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014).

Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,* (New York: Doubleday, 1989).

Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Broadway Books, 2015).