GREAT DECISIONS
1918 • FOREIGN POLICY ASSOCIATION 2019 EDITION

Cyber Conflict and geopolitics

Acronyms and abbreviations

DHS—Department of Homeland Security

CCP—Chinese Communist Party

GDP—gross domestic product

IP—intellectual property

IRA—Internet Research Agency

NATO—North Atlantic Treaty Organization

WWI—World War I

WWII—World War II

Glossary

Alfred Mahan: American naval theorist who wrote about the relationship between maritime technology and power and wealth in European countries.

Cyber espionage: Using computer networks to spy or to illegally obtain confidential information.

Cyberspace: The connections and communications between computer networks.

Doxing: Maliciously publishing on the Internet private information that identifies individuals or organizations without consent.

Geopolitics: the effect that geography has on politics and international relations.

Gerasimov Doctrine: Named for General Valery Gerasimov, who published an article in 2013 describing Russian strategy of using hacking to destablize an enemy.

Halford Mackinder: British geographer who wrote about rail technology increasing European countries' land power.

Hardware: Physical parts of a computer, such as the monitor, central processing unit and keyboard.

Hillary Clinton: Former U.S. Secretary of State who publicly supported Internet freedom worldwide.

Intellectual property: Intangible creations and materials, such as trade secrets.

Internet Research Agency: Created in 2013 by Vyacheslav Volodin, it is a company that supports Russian interests through fake online interactions and accounts on social media and other websites. Major campaigns include influencing the 2016 U.S. election and foreign policy in Ukraine and the Middle East.

James Clapper: Director of National Intelligence from 2010 to 2017 who testified that he was not confident in the United States' cyber defense capabilities, specifically against Russia.

James Comey: Director of the Federal Bureau of Investigation from 2013 until 2017 who stated that most U.S. companies, whether they knew it or not, had been hacked by China.

Li Bingyan: Chinese Major General who argued that China's cyber proficiencies and policies were an effective counter to American power in the world.

Malware: Malicious software. An example is the Stuxnet worm.

Michael Rogers: Commander of the U.S. Cyber Command from 2014 to 2018 who reported that the United States was extremely vulnerable to cyberattacks from other countries, specifically China.

Robert Mueller: Director of the Federal Bureau of Investigation from 2001 to 2013. In 2016, he indicted several Russians for their influence on the 2016 elections through fake online accounts.

Software: The data within the computer, such as programs or information within the systems.

Stuxnet: A malware "worm" allegedly designed by Israel and the United States to damage Iran's nuclear program through targeting their nuclear centrifuges.

Tom Donohue: Current President of the U.S. Chamber of Commerce, he has stated that a trade war would threaten the economy.

U.S. Cyber Command: Under the Department of Defense, this command focuses on protecting American interests through cyberspace.

Vyacheslav Volodin: Current Russian politician and former aide to Russian president Vladimir Putin. He created the Internet Research Agency to influence social media to suit Russia's interests.