The Issue

Cyberspace is a new domain of conflict, one guided by few accepted rules or standards of behavior. Policymakers find offensive cyber operations attractive because they are relatively inexpensive, can be designed to be less destructive than kinetic strikes (i.e., those against physical targets), and can provide a high degree of anonymity to the attacker. The vast majority of these operations includes cyber espionage (theft of military and political secrets or intellectual property) and political disruptions (website defacement or distributed denial of service [DDoS] attacks that flood a website with so much data that it can no longer respond).

The White House's 2011 International Strategy for Cyberspace warns that "the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." However, although experts generally assume that a cyberattack that caused death or physical destruction would be considered an armed attack, the threshold for a military response to other forms of cyberattack remains uncertain. Indeed, cyberspace is marked by high strategic instability. Defending against cyber threats is extremely difficult. Would-be defenders need to worry about millions of lines of computer code, hundreds of devices, and scores of networks, but an attacker need find only one vulnerability.

Moreover, attribution of cyberattacks is difficult and slow, which makes them different from other weapons. Attackers can hide their tracks with relative ease, and the attacks can happen in minutes, if not seconds. Many countries rely on proxies, criminal groups, or patriotic hackers to conduct operations: even if the location of the hackers can be determined, anyone anywhere could have authorized the attack. This conundrum greatly complicates efforts to retaliate and prevent attacks.

Successful attacks are also likely to risk escalation. If, based on past trends, military leaders fear that their networks or weapons systems could be subjected to cyberattacks—which would limit their ability to order forces in the field or to launch weapons—they would have an incentive to use their weapons systems preemptively; such a move would escalate and further destabilize a conflict.

China, Taiwan, Vietnam, Malaysia, Brunei, and the Philippines have competing territorial claims in the South China Sea. In recent years, China has exerted authority over the area by increasing the size of existing islands or creating new ones, as well as by constructing ports, military installations, and airstrips. The United States has promoted the right of military vessels to operate in China's claimed two-hundred-mile exclusive economic zone and has rejected China's claim to a twelve-mile territorial zone around the artificial islands it has built. Since 2015, the United States has signaled its opposition by flying military aircraft and sending U.S. Navy ships near certain islands.

Last week, the U.S. Air Force conducted a flight near a shoal claimed by China in the South China Sea. Three days later, the Nasdaq Stock Market suffered a hack that damaged computers and forced the suspension of trading for two days, imposing significant costs on various U.S. companies and denting confidence in the U.S. financial system. The Zheng He Squadron, an underground hacker collective based in China, has claimed responsibility for the hack. The group has known ties to the People's Liberation Army, China's military. U.S. intelligence agencies assess with 90 percent certainty that the hack occurred with the knowledge or support

of parts of the Chinese government. Beijing, however, claims no knowledge of the attack. The president has convened the National Security Council to discuss how the United States should respond.

Background

The rapid diffusion of information technology has remade economics, politics, and international affairs. It has transformed commerce, making global supply chains possible and generating enormous wealth. It has created social and cultural networks that span the globe, enabling people to overcome distance and share knowledge and ideas. It has provided powerful tools for political organization and protest.

The digital revolution has also created new sources of vulnerability. States, terrorists, and criminals can shut down power, communication, transportation, and financial networks with the click of a mouse, inflicting not just massive economic losses but also death and physical destruction.

The transparency and verification processes that help limit nuclear competition—which deal with physical weapons, materials, and facilities—do not appear to apply to digital weapons. Counting or controlling malware is practically impossible. Moreover, no shared understanding of the rules of state behavior in cyberspace exists—whether, for example, a country is justified in responding to cyberattacks with conventional military force. Major powers, including the United States and China, have been willing to discuss the threats in cyberspace but have been slow to develop a policy framework.

After years of silence, the U.S. government has gradually become more transparent about its development and use of cyberattacks. The 2015 Defense Department cyber strategy, for example, explicitly recognizes offensive missions, directing the Pentagon to develop cyber capabilities that can support military operations. Although experts widely believe that the United States and Israel were behind Stuxnet, the malicious software (malware) designed to slow Iran's nuclear program by damaging centrifuges at the Natanz nuclear facility in 2009, the United States did not admit any role. In fact, the first public acknowledgment of a U.S. use of cyber weapons came in February 2016, when Pentagon officials announced that U.S. Cyber Command had launched attacks against the self-proclaimed Islamic State. Cyber Command has grown from approximately nine hundred personnel to more than six thousand, and requests for cyber operations in the 2019 defense budget totaled $8.5 billion, an increase of more than 25 percent from 2017.

China and the United States have a history of clashes in cyberspace. According to a *Washington Post* report, Chinese hackers have stolen information relating to more than two dozen U.S. weapons programs, including the Patriot missile system, the F-35 Joint Strike Fighter, and the U.S. Navy's new littoral combat ship. The White House, the State Department, the Office of Personnel Management, and NASA have been breached. Attacks on Adobe, Disney, DuPont, General Dynamics, General Electric, Google, Johnson & Johnson, Juniper Networks, Sony, Symantec, and Yahoo have also been publicly reported, and Chinese hackers have reportedly targeted the negotiation strategies and financial information in energy, banking, law, and other sectors.

In response to U.S. claims of Chinese hacking, China has noted that it is also a victim of cybercrime and that the majority of attacks against it originates from internet protocol (IP) addresses in the United States, Japan, and South Korea. Chinese media were quick to echo claims by the former National Security Agency contractor Edward Snowden that the United States hacks targets on the Chinese mainland and in Hong Kong.

In April 2015, President Barack Obama signed an executive order that declared a national emergency to deal with the threat of "significant malicious cyber-enabled activities," allowing for economic sanctions against companies or individuals that profited from cyber theft. The order threatened to block financial transactions routed through the United States, prevent exports to the United States, and prevent executives of the companies that benefit from the hacks from traveling to the United States.

In August 2015, the *Washington Post* reported that the Obama administration planned to levy these sanctions against Chinese companies in the lead-up to the summit the following month between Presidents Barack Obama and Xi Jinping. Perhaps because of the threat, the summit produced a breakthrough agreement. Both sides agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." Washington and Beijing also agreed to identify and endorse norms of behavior in cyberspace and to establish two high-level working groups and a hotline between them. After departing the United States, Xi signed similar agreements with the United Kingdom and at a Group of Twenty (G20) meeting in Turkey.

Following the presidents' September summit, the cybersecurity firm FireEye reported a sharp decline in the number of Chinese cyberattacks but suggested that actors could simply have become stealthier and more difficult to detect. U.S. Assistant Attorney General John P. Carlin confirmed the company's findings that attacks were "less voluminous but more focused, calculated, and still successful."

The U.S.-China group on security issues met only once before the end of the Obama administration, but the cybercrime group reported some progress. The two sides established a point of contact and a designated email address, and successfully cooperated on taking down websites with false information. After Donald J. Trump met Xi Jinping in April 2017, Washington and Beijing agreed to a U.S.-China Comprehensive Dialogue that would have four pillars, including one on law enforcement and cybersecurity.

Role of the United States

The United States has an interest in ensuring that China does not assert its sovereignty claims over the South China Sea by using force or intimidation. Washington has sought to secure its interest through freedom of navigation operations—sending ships or aircraft into areas that China claims but that the United States considers open to all—as well as increased military exercises with its friends and allies in the region. The United States also has an interest in defining the rules of behavior for cyberspace, where it has tried to strengthen deterrence by building up offensive capabilities, demonstrating its ability to attribute attacks, and indicting foreign hackers. It has also promoted norms of behavior through bilateral agreements and multilateral forums.

The principal policy options available in this case are discussed below. These responses are available individually, in combination, or all together.

Cyber responses. The United States could pursue a proportionate response that tries to disrupt critical networks within China, such as its banking system, for a limited period. The attacks could also be directed at a target that seems particularly valuable to the Chinese leadership, such as the censorship technology that constitutes the so-called Great Firewall. The U.S. response should be accompanied by some level of attribution, meaning that the United States would need to identify the attackers, and the attack would reveal some of the United States' technical and intelligence capabilities.

With this option, the United States would essentially be responding in kind, keeping the U.S.-China dispute in the domain (cyberspace) it is already in rather than extending it. Thus, even if the conflict were to escalate, Washington could claim that it was not the instigator. Moreover, the United States would likely be capable of mounting a targeted cyberattack that stood a good chance of producing the desired effect.

Nonetheless, a cyber response has costs and risks. A cyberattack might fail if the defender has already patched the vulnerability. Given China's extensive connection with the global economy, malware used against China could also quickly spread to the rest of world, infecting U.S. allies and eventually making its way back to the United States. Although limited to one domain, cyberattacks could also escalate rapidly. If attacks damage Chinese defense networks and command-and-control nodes, Beijing could fear that a conventional strike might soon follow and decide to launch conventional strikes on U.S. military assets as quickly as possible. Chinese economic retaliation against the United States is also possible. In addition, other countries could find U.S. claims of China's guilt unconvincing. Failing to convince others that the Chinese government was behind the attacks would not only limit support for the U.S. response but also undermine Washington's efforts to develop international norms for behavior in cyberspace.

Punitive sanctions. In April 2015, Obama issued an executive order that laid the groundwork for economic sanctions. Declaring a national emergency to deal with the threat of "significant malicious cyber-enabled activities," the order enabled the Treasury secretary to sanction individuals and entities involved, directly or indirectly, in cyberattacks. Possible sanctions include freezing their financial assets and barring commercial transactions with them. In the current scenario, the White House could sanction high-level Chinese authorities who it believes ordered the attack and levy economic sanctions on government entities and state-owned enterprises deemed to be connected to the hacks. It could also expel Chinese diplomats from the United States.

Another response would be to indict the individual hackers involved. Although these individuals are unlikely to ever be handed over to U.S. authorities for trial, their international travel would be limited, and the indictments could deter future Chinese hackers who wish to someday travel abroad. As with the cyber response, punitive sanctions would involve identifying the attackers and revealing some U.S. technical and intelligence methods.

It could take a while for economic sanctions to be imposed; it could take even longer for them to bite and affect the target's behavior. Chinese firms could also skirt financial restrictions by trading with Russia or others, and China could retaliate against U.S. companies that heavily export to China. The U.S. response could appear feckless, undermine deterrence, and embolden

other cyberattackers. As with a cyber response, the United States would need to convince others that the Chinese government was behind the attacks. Otherwise, support for U.S. sanctions would be limited, possibly reducing their effectiveness.

Military responses. Washington could increase freedom of navigation operations and the U.S. military presence more broadly in the South China Sea. It would help small states build maritime law enforcement and security capacity and in particular improve the Philippines' long-term maritime capabilities. The United States would also expand military exercises with states in the region.

Such a response is clear and well within the capability of the U.S. military and would also convey the United States' resolve. Washington could announce that its military initiatives were in response to the Chinese cyberattacks, or it could refrain from doing so. Connecting the response to the attack publicly might be more escalatory but would have the advantage of marking a clear response to the Chinese behavior, ideally leading Beijing to reduce or end this activity. Not making the connection public would be less provocative but could signal to potential attackers that cyberattacks such as the one against Nasdaq fall below the threshold for a forthright response. Regardless of whether the United States announces the connection, military steps could escalate Chinese reclamation behavior in the South China Sea or lead to an incident that escalates into military conflict. Moreover, U.S. support could also embolden the smaller states to push China harder than they would dare to alone.

Research and Preparation

Your role sheet contains three parts: a description of your role, issues for consideration, and research leads. The role description details the position you will portray in the role-play. The issues for consideration will guide your thinking and assist you in approaching the case from the perspective of your assigned role. Most relevant, however, are the research leads. Going beyond the reports and articles linked to throughout the case and in the reading list, these research leads provide suggested materials and topics for further research specifically relevant to your assigned role. Below are some tips to review as you prepare for the role-play exercise.

Research and Preparation

- Draw on the case notes, additional case materials, and your own research to familiarize yourself with
    - the goals of the NSC in general and of this NSC meeting in particular;
    - the U.S. interests at stake in the case and their importance to national security;
    - your role and your department or agency, including its purpose and objectives in the government and on the NSC;
    - the aspects of the case most relevant to your role;
    - the elements that a comprehensive policy proposal on the case should contain; and
    - the major debates or conflicts likely to occur during the role-play. You need not resolve these yourself, of course, but you will want to anticipate them in order to articulate and defend your position in the NSC deliberation.
- Set goals for your research. Know which questions you seek to answer and refer back to the case notes, additional readings, and research leads as needed.
- Make a list of questions that you feel are not fully answered by the given materials. What do you need to research in greater depth? Can your classmates help you understand these subjects?

- Using the case materials, additional readings, and discussions with your classmates, weigh the relative importance of the U.S. interests at stake in the case. Determine where trade-offs might be required and think through the potential consequences of several different policy options.
- Conduct your research from the perspective of your assigned role, but be sure to consider the full range of U.S. interests at stake in the case, whether diplomatic, military, economic, environmental, moral, or otherwise. This will help you strengthen your policy position and anticipate and prepare for debates in the role-play.
- Consider what questions or challenges the president or other NSC members might raise regarding the options you propose and have responses ready.

Sources

- Consult a wide range of sources to gain a full perspective on the issues raised in the case and on policy options. Seek out sources that you may not normally use, such as publications from the region(s) under discussion, unclassified and declassified government documents, and specialized policy reports and journals.
- Remember: Wikipedia is not a reliable source, but it can be a reasonable starting point. The citations at the bottom of each entry often contain useful resources.
- Just as policymakers tackle issues that are controversial and subject to multiple interpretations, so will you in your preparation for the writing assignments and role-play. For this reason, evaluate your sources carefully. Always ask yourself:
    - When was the information produced? Is it still relevant and accurate?
    - Who is writing or speaking and why? Does the author or speaker have a particular motivation or affiliation that you should take into account?
    - Where is the information published? Determine the political leanings of journals, magazines, and newspapers by reading several articles published by each one.
    - Who is the intended audience?
    - Does the author provide sufficient evidence for his or her analysis or opinion? Does the author cite reliable and impartial sources?
    - Does the information appear one-sided? Does it consider multiple points of view?
    - Is the language measured or inflammatory? Do any of the points appear exaggerated?
- Take note of and cite your sources correctly. This is important not just for reasons of academic integrity, but so that you can revisit them as needed.
- Ask your teacher which style he or she prefers you use when citing sources, such as Modern Language Association (MLA), Chicago Manual of Style, or Associated Press (AP).

Reading List

2.1 The Issue

Ian Bremmer, "These 5 Facts Explain the Threat of Cyber Warfare," *Time*, June 19, 2015, http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare.

"Fact Sheet: The Department of Defense (DOD) Cyber Strategy," Department of Defense, April 2015, http://defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf.

"Why Is the South China Sea Contentious?" BBC News, July 12, 2016, http://bbc.com/news/world-asia-pacific-13748349.

2.2 Background

Jose Pagliery, "The Inside Story of the Biggest Hack in History," CNN Money, August 5, 2015, http://money.cnn.com/2015/08/05/technology/aramco-hack.

David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *New York Times*, February 16, 2016, http://nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

Kathrin Hille, "Chinese Tech Companies Have Army-Linked 'Cybermilitias,'" CNN, October 12, 2011, http://cnn.com/2011/10/12/business/china-tech-cyber-crime/index.html.

2.3 Role of the United States

"Fact Sheet: Cybersecurity National Action Plan," Office of the White House Press Secretary, February 9, 2016, http://whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

David E. Sanger, "U.S. Wrestles With How to Fight Back Against Cyberattacks," *New York Times*, July 30, 2016, http://nytimes.com/2016/07/31/us/politics/us-wrestles-with-how-to-fight-back-against-cyberattacks.html?_r=0.

Henry Farrell, "Promoting Norms for Cyberspace," Council on Foreign Relations, April 2015, http://cfr.org/cybersecurity/promoting-norms-cyberspace/p36358.

Further Reading

Graham Allison, "The Thucydides Trap: Are the U.S. and China Headed for War?" *Atlantic*, September 24, 2015, http://theatlantic.com/international/archive/2015/09/united-states-china-war-thucydides-trap/406756.

Aria Bendix, "Trump Signs a Long-Awaited Cybersecurity Order," *Atlantic*, May 11, 2017, https://www.theatlantic.com/news/archive/2017/05/trump-signs-cybersecurity-order-hacking-election/526407/.

Chris Bing, "Chinese hackers starting to return focus to U.S. corporations," CyberScoop, November 6, 2017, https://www.cyberscoop.com/keyboy-dde-pwc-microsoft-word-rtf/.

Adam Blenford and Christine Jeavans, "After Snowden: How Vulnerable Is the Internet?" *BBC News*, January 27, 2014, http://bbc.com/news/technology-25832341.

Christopher Brank, Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival*, April 1, 2013, https://www.iiss.org/en/publications/survival/sections/2013-94b0/surviv….

Adrian Chen, "The Agency," *New York Times Magazine*, June 7, 2015, http://nytimes.com/2015/06/07/magazine/the-agency.html.

"Cybersecurity Law of the People's Republic of China," Council on Foreign Relations, July 6, 2015, http://dev-www.cfr.org/internet-policy/cybersecurity-law-peoples-republic-china/p36788.

Simon Denyer and Emily Rauhala, "Beijing's Claims to South China Sea Rejected by International Tribunal," *Washington Post*, July 12, 2016, http://washingtonpost.com/world/beijing-remains-angry-defiant-and-defensive-as-key-south-china-sea-tribunal-ruling-looms/2016/07/12/11100f48-4771-11e6-8dac-0c6e4accc5b1_story.html.

"Five Things to Know: The Administration's Priorities on Cybersecurity," National Archives and Records Administration**,** https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity.

Bonnie S. Glaser, "Armed Clash in the South China Sea," Council on Foreign Relations, April 2012, http://cfr.org/asia-and-pacific/armed-clash-south-china-sea/p27883.

Andy Greenberg, "China tests the limits of its U.S. hacking truce," *Wired*, October 31, 2017, https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/

Brian Michael Jenkins, "Cyberterrorism and the Role of Silicon Valley," *Rand blog*, June 13, 2016, http://rand.org/blog/2016/06/cyberterrorism-and-the-role-of-silicon-valley.html.

Sarah Kreps and Debak Das, "Americans are united on retaliating against Russian cyberattacks," *Washington Post*, January 19, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/01/19/americans….

Eric Lipton, David E. Sanger and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S," *New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Ewen MacAskill and Rajeev Syal, "Cyber-attack on UK parliament: Russia is suspected culprit," Guardian, June 25, 2017, https://www.theguardian.com/politics/2017/jun/25/cyber-attack-on-uk-parliament-russia-is-suspected-culprit.

Mark McDonald, "Adding More Bricks to the Great Firewall of China," *New York Times*, December 23, 2012, http://rendezvous.blogs.nytimes.com/2012/12/23/adding-more-bricks-to-the-great-firewall-of-china.

Barack Obama, "Taking the Cyberattack Threat Seriously," *Wall Street Journal*, July 19, 2012, http://wsj.com/articles/SB10000872396390444330904577535492693044650.

Nicole Perlroth and Michael Corkery, "North Korea Linked to Digital Attacks on Global Banks," *New York Times*, May 26, 2016, http://nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html.

Nicole Perlroth, "Among Digital Crumbs from Saudi Aramco Cyberattack, Image of Burning U.S. Flag," *Bits* (blog), *New York Times*, August 24, 2012, http://bits.blogs.nytimes.com/2012/08/24/among-digital-crumbs-from-saudi-aramco-cyberattack-image-of-burning-u-s-flag.

"Remarks by the President at the Cybersecurity and Consumer Protection Summit," Office of the White House Press Secretary, February 13, 2015, http://whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

"Sanctions Related to Significant Malicious Cyber-Enabled Activities," U.S. Department of the Treasury, last updated December 31, 2015, http://treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx.

David E. Sanger and Nicole Perlroth, "N.S.A Breached Chinese Servers Seen as Security Threat," *New York Times*, March 22, 2014, http://nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

Bruce Schneier, "The Story Behind the Stuxnet Virus," Forbes, October 7, 2010, http://forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html.

Adam Segal, "Cyberspace Governance: The Next Step," Council on Foreign Relations, March 2011, http://cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

Adam Segal, "An Update on U.S.-China Cybersecurity Relations," CFR Net Politics blog, November 17, 2017, https://www.cfr.org/blog/update-us-china-cybersecurity-relations.

Scott Shane et al, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core," *The New York Times*, November 12, 2017, https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html?_r=0.

Amar Toor, "The U.S. is Dropping 'Cyberbombs' on ISIS," Verge, April 25, 2016, http://theverge.com/2016/4/25/11501062/us-cyberattack-isis-cyber-command-nsa.

"Vietnam-linked hackers likely targeting Philippines over South China Sea dispute: FireEye," Reuters, May 25, 2017, http://www.reuters.com/article/us-cyber-philippines-southchinasea-idUSK….

Derek Watkins, "What China Has Been Building in the South China Sea," *New York Times*, last updated February 29, 2016, http://nytimes.com/interactive/2015/07/30/world/asia/what-china-has-been-building-in-the-south-china-sea-2016.html?_r=0.

Richard Wike, “6 Facts About How Americans and Chinese See Each Other,” Pew Research Center, March 30, 2016, http://pewresearch.org/fact-tank/2016/03/30/6-facts-about-how-americans-and-chinese-see-each-other.

Sam Wainwright, “Revolutionary Communication Innovations,” CNN, June 10, 2011, http://globalpublicsquare.blogs.cnn.com/2011/06/10/how-connectedness-is-spurring-innovation.

Kim Zetter, “The NSA Acknowledges What We All Feared: Iran Learns From U.S. Cyberattacks,” *Wired*, February 10, 2015, http://wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks.