Resources from the Council on Foreign Relations

(from a different but similar simulation case)

2.2 Context

The United States and China have significant disagreements over cyber espionage, cyberattacks, and internet governance. These differences have intensified in recent years as cyber issues have become more significant on the bilateral and global agenda.

Several prominent cyberattacks over the last two decades have driven increased attention to cyberspace. In late 2009 or early 2010, Iran replaced about one thousand of the nine thousand centrifuges deployed at its fuel enrichment plant at Natanz. The centrifuges had been damaged by sophisticated malware, eventually known as Stuxnet, which was allegedly developed and launched by the United States and Israel to slow down Iran's nuclear program. The Natanz plant seriously concerned those two countries because its centrifuges were producing enriched uranium, which can, if properly processed, be used in a nuclear weapon. Sometime in the summer of 2010, Stuxnet escaped into the wild, eventually spreading to more than 115 countries, though it did no damage to other systems. Washington also reportedly developed a cyberattack plan, code-named Nitro Zeus, to be used if negotiations failed to limit Tehran's nuclear program and military conflict erupted. U.S. Cyber Command reportedly planned attacks on air defenses, communications, and parts of the power grid. The United States, Iran, and other powers reached a deal over Iran's nuclear program in 2015, and the apparent cyberattack plan has never been used.

After Stuxnet was discovered, Iran retaliated with its own cyberattacks. Between September 2012 and June 2013, an activist group called Izz ad-Din al-Qassam Cyber Fighters took credit for roughly two hundred DDoS attacks on almost fifty Western financial institutions, including Capital One, CitiGroup, HSBC, JPMorgan Chase, PNC, SunTrust, U.S. Bancorp, and Wells Fargo. These attacks made websites unavailable for a few hours but did not threaten the integrity of the financial system.

In August 2012, a virus, known as Shamoon, struck Saudi Aramco, Saudi Arabia's state-owned oil company, which supplies about a tenth of the world's oil. Shamoon corrupted tens of thousands of hard drives and shut down the employee email service. The company had to replace thirty thousand computers, but the malware did not affect systems involved with technical oil operations. A subsequent attack damaged RasGas, a joint venture between Qatar Petroleum and ExxonMobil. Data was destroyed, but production continued. A group calling itself the Cutting Sword of Justice claimed responsibility, but, in this case, as in the earlier financial attacks, U.S. officials speaking off the record blamed the Iranian government. Predominantly Sunni Saudi Arabia and predominantly Shiite Iran often compete for influence and leadership in the Middle East.

During Thanksgiving week in 2014, employees of Sony Pictures lost access to the company's computer networks and their email accounts due to a massive hack. The hackers, operating under the name Guardians of Peace, not only stole one hundred terabytes of internal data but also damaged two-thirds of the company's servers and computers. On December 19, 2014, the FBI announced that the Guardians of Peace were North Korean government hackers. Pyongyang had previously expressed outrage over the Sony film *The Interview*, which depicts the assassination of its supreme leader, Kim Jong-un. This was the first time the U.S. government had explicitly and directly named another government as responsible for hacking.

On January 2, 2015, the United States levied economic sanctions on the Reconnaissance General Bureau, a North Korean intelligence agency; the Korea Tangun Trading Corporation, which acquires military-related materials and technology for North Korea; and the Korea Mining Development Trading Corporation, the country's main exporter of ballistic missiles and conventional weapons. The United States also reportedly asked the Chinese government for help with identifying and controlling North Korean hackers, some of whom were reportedly based in a hotel in northeastern China, but public statements from China were noncommittal. Around this time, North Korea disappeared from the internet. A DDoS attack knocked offline the few North Korean websites available to the outside world. Despite some suspicion that the U.S. government was responsible, the attack was more likely conducted by individual hackers or a group of activists.

In March 2016, the United States indicted seven Iranians working for entities affiliated with the Islamic Revolutionary Guard Corps for conducting cyberattacks in 2012 and 2013 against the U.S. financial sector, also charging one of them with unauthorized access to the control systems of a New York dam. The United States also announced that Cyber Command undertook offensive operations against the Islamic State. According to the *New York Times*, U.S. military hackers first placed "implants" in the militants' networks to learn about commanders, then began to alter messages to make fighters more vulnerable to attack by U.S. drones. In other cases, Cyber Command disrupted the Islamic State's financial transactions.

The 2016 U.S. presidential election was marked by repeated hacking incidents. In July, thousands of emails from the Democratic National Committee (DNC) were leaked and subsequently published by WikiLeaks. The fallout was significant, leading to the resignations of DNC Chairwoman Debbie Wasserman Schultz, representative from Florida, and many top party aides. In the fall of 2016, thousands of emails from the personal Gmail account of John Podesta, the chairman of Hillary Clinton's presidential campaign, were also released. Researchers concluded that hackers linked to Russian intelligence were behind both the DNC and the Podesta hacks. The U.S. government also denounced the incidents as Russia-directed hacking, accusing Russia of attempting to interfere in U.S. elections. In December 2016, the White House announced that it was expelling thirty-five Russian spies from the United States and sanctioning nine individuals and organizations linked to the hacking: the Federal Security Service and the Russian military intelligence agency, known as GRU; four intelligence officers; and three companies that provided material support to the hackers.

As cyber issues have expanded in scope and scale, the United States has begun to coordinate attribution and indictments with its allies and partners. In February 2018, the White House and the United Kingdom foreign ministry blamed Russia for the NotPetya attack, a ransomware attack that caused hundreds of millions of dollars in damage to businesses in Ukraine and Europe. In December of the same year, the United States, Australia, Canada, and the United Kingdom blamed North Korea for the 2017 WannaCry ransomware attack.

In late 2019 or early 2020, a group of hackers hid a piece of malware in a widely used network management software made by the company Solar Winds, allowing them to gain access to the networks of some eighteen thousand companies and government agencies that installed the software. The hacking campaign ran undetected until December 2020, when the cybersecurity firm FireEye detected the attack and announced that it had been among the targets. Although most of the companies that had installed the infected software had not suffered any data theft from the hack, analysts assess that hackers stole data from at least one hundred companies and nine U.S. government agencies. U.S. intelligence agencies determined that the campaign, which represented one of the most extensive cyberattacks on the United States to date, was likely conducted by Russian hackers. In April 2021, President Joe Biden announced new economic sanctions against several Russian financial institutions and technology companies in response to the attack.

Ransomware attacks have become a growing concern for countries in recent years, increasing by 148 percent globally between 2019 and 2020. In May 2021, a ransomware attack on Colonial Pipeline forced the company to shut down operations, resulting in fuel shortages along the eastern seaboard of the United States. DarkSide, a criminal group based in Russia, was behind the attack and soon disbanded as public outrage grew. Soon after the attack, the Biden administration released an executive order designed to improve the federal government's cyber posture by ensuring agencies use two-factor authentication and encrypt data at rest. It also created a Cybersecurity Safety Review Board, which will include federal officials from the Department of Defense, the Department of Justice, the Cybersecurity and Infrastructure Security Agency (CISA), the NSA, the FBI and the private sector to analyze and make recommendations after significant cyber incidents.

With cyberattacks growing in frequency and sophistication, governments have sought to establish norms that could govern cyberspace. Since 2005, a small group of governmental experts has gathered at the United Nations to discuss cyber threats. The group, which includes government representatives from the United States, China, and Russia, signed a nonbinding report [PDF] in 2013 agreeing that international law applies in cyberspace. This means, among other things, that cyberattacks can be considered a use of force, that a country can exercise the right to self-defense if it is the victim of a cyberattack, and that the laws of armed conflict apply to cyberwar. The 2013 report also asserted that countries are responsible for and should act against cyberattacks that originate within their territories. In 2015, the same group agreed to a set of peacetime norms [PDF] promoted by the United States. Those norms include the idea that countries should not attack each other's critical infrastructure or target each other's computer emergency response teams—national agencies that defend against and help recover from cyberattacks. The norms also hold that countries should assist other nations investigating cyberattacks and cybercrime. However, the 2017 round of negotiations ended with the participants unable to identify new norms or agree how to apply international law to cyberspace. In November 2018, the United States, alongside China, North Korea, and Russia, refused to sign an agreement promoted by the French government and Microsoft calling for governments and companies to adhere to common principles designed to limit offensive cyberattacks.

After the failure of the 2017 meeting to reach a consensus, the norms discussion at the United Nations split into two parallel paths. In addition to the representatives from twenty-five selected member states who are part of the group of government experts, a 2018 Russian resolution [PDF] in the General Assembly established the Open-Ended Working Group (OEWG) on international cybersecurity. With the goal of being a "more democratic, inclusive, and transparent" forum for the discussion and monitoring of cyber norms, the OEWG involves all UN member states. Some analysts have criticized Moscow's formation of a larger group, suggesting that it was in part a deliberate effort to make consensus more difficult. However, the OEWG has seen widespread participation by countries and nongovernmental organizations, making it a potential tool to build confidence, transparency, and communication among countries in their pursuit of cyber norms.

In March 2021, the OEWG reached a consensus on a nonbinding report [PDF]. Although it offered little in the way of new progress on cyber norms, the report represented a successful break in a years-long diplomatic stalemate and a success for the OEWG as a forum for cooperation on cyber issues. Most notably, the report reaffirmed the 2015 recommendations on cyber norms and international law established by the group of governmental experts and acknowledged the need for further progress on other emerging issues that have so far seen little international discussion, including protecting health-care systems and other critical infrastructure and using cyberspace to interfere with other countries' electoral processes. Although the report does not offer recommendations on how to address these topics, their inclusion could lay the groundwork for future cooperation on international cyber norms.

Recent History

Chinese cyberattacks in particular are often driven by the desire to collect political and military intelligence. According to a 2013 *Washington Post* report, Chinese hackers have stolen information relating to over 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 State Department, the White House, the Office of Personnel Management, and NASA have been breached. China's cyber espionage, however, has not been limited to U.S. targets. Embassies, foreign ministries, and the government offices of Germany, India, Indonesia, Romania, South Korea, and Taiwan, among others, have also been breached.

The need to move Chinese industries out of labor-intensive, energy-inefficient, highly polluting manufacturing sectors to cleaner, more technology-intensive ones also motivates cyberattacks. The Chinese fear being caught in a technology trap, dependent on U.S., Japanese, and European firms for core technologies. Cyberattacks are intended to acquire information that could help Chinese firms develop such technologies themselves. Attacks on Adobe, Disney, Dupont, General Dynamics, General Electric, Google, Johnson & Johnson, Juniper Networks, Symantec, and Yahoo have been publicly reported. Chinese hackers have also reportedly targeted the negotiation strategies and financial information of 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, with the majority of attacks originating from internet protocol (IP) addresses in the United States, Japan, and South Korea. The Chinese press was quick to echo claims by National Security Agency (NSA) contractor Edward Snowden that the United States hacks targets on the Chinese mainland and in Hong Kong.

Chinese cyber strategy has a military dimension as well. PLA analysts write frequently of seizing information dominance early on in a conflict by conducting cyberattacks on an enemy's command and control centers. These centers allow commanders to collect information, issue orders, and monitor operations. Follow-up attacks would target transportation, communication, and logistics networks to slow down an adversary. To prepare for this strategy in any potential conflict with the United States, Chinese actors appear to be surveilling and entering military networks as well as some critical U.S. infrastructure, such as power grids and oil and gas pipelines. U.S. military doctrine—in particular the Air-Sea Battle doctrine (now known as Joint Concept for Access and Maneuver in the Global Commons), adopted to defeat cruise missiles, submarines, and cyber capabilities—also assumes cyberattacks on an adversary's sensors, networks, launchers, and weapons in the beginning stages of a conflict.

As with economic policy and national security, Chinese President Xi Jinping has consolidated control over cybersecurity by creating a so-called small leading group, an ad hoc body that advises the Politburo and implements decisions. Moreover, on December 31, 2015, China's Central Military Commission overhauled the organizational structure of the PLA, establishing three new branches. One of them is the Strategic Support Force, whose operations remain unclear but whose responsibilities reportedly include intelligence, technical reconnaissance, electronic warfare, cyber offense and defense, and psychological warfare.

Beginning in 2013, Washington publicly increased pressure on Beijing over cyber espionage. In March 2013, for example, National Security Advisor Tom Donilon spoke of the "serious concerns

about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale." Two months later, the Defense Department went further and, in a break from the past, directly blamed the Chinese government and military for espionage.

In May 2014, the Department of Justice charged five Chinese hackers with stealing the business plans, internal deliberations, and other intellectual property of Westinghouse Electric, U.S. Steel Corporation, and other companies. The department claimed the hackers were members of the PLA's General Staff, Third Department, Unit 61398, located in Shanghai. The indictment incensed the Chinese government, which quickly suspended a high-level bilateral cyber working group.

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 from 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 Obama and Xi. Perhaps because of the threat, the summit produced a breakthrough agreement. Both sides pledged 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 establish two high-level working groups and a hotline between the two sides. After departing the United States, Xi signed similar agreements with the United Kingdom and at the Group of Twenty meeting in Turkey.

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

The U.S.-China group on security issues only met once before the end of the Obama administration, but the cybercrime group reported some small progress. The two sides established a point of contact and a designated email address and successfully cooperated on taking down fake websites. After Presidents Donald Trump and Xi Jinping met at Mar-a-Lago 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. The negotiations broke down, however, before the two countries could come to an agreement.

In 2018, the Trump administration implemented a series of sweeping tariffs on Chinese goods, citing unfavorable trade practices and Chinese theft of American intellectual property. The resulting trade war stalled cooperation on cybersecurity and, according to cybersecurity firms, is correlated positively with an increase in cyberattacks on American businesses and government agencies. In December, the United States, along with Australia, Canada, New Zealand, and the United Kingdom, called out Chinese cyber operations, and the U.S. Department of Justice announced the indictment of two Chinese hackers associated with the Ministry of State Security.

In September 2018, the Trump administration announced that it would adopt a more aggressive cybersecurity strategy that authorized using offensive cyber operations as a deterrent against foreign cyberattacks. Under the 2018 Defense Department Cyber Strategy [PDF], U.S. Cyber Command adopted a new, more offensive strategy known as defend forward, which focuses on observing, countering, and disrupting adversary operations before they affect U.S. networks. The Trump administration further oversaw the creation of CISA within the Department of Homeland Security to coordinate and improve government defenses against cyberattacks. Despite this increase in offensive operations, a 2019 U.S. Senate report [PDF] concluded that critical U.S. government agencies remained dangerously unprepared to defend against cyberattacks. The 2020 Solar Winds hack that gave hackers access to the networks of several federal agencies has further underscored those vulnerabilities and the need to bolster U.S. cyber defenses.

Upon taking office in January 2021, Biden has reaffirmed the importance of cyber issues to U.S. national security and signaled plans to improve U.S. cyber defenses, increase efforts to deter cyberattacks by imposing costs on perpetrators, and invigorate diplomatic efforts toward cyber norms. As of April 2021, early budget proposals by the Biden administration have moved to increase funding to CISA and provide nearly $1 billion to go toward modernizing government technology systems.

Meanwhile, tensions between the United States and China have remained high. In March 2021, Microsoft warned that a Chinese state-sponsored group was responsible for infecting tens of thousands of Exchange servers. The first round of high-level talks between Washington and Beijing since Biden's inauguration were marked by tense rhetoric and yielded little progress toward reducing tensions between the two countries or addressing ongoing issues including cyber concerns. In April 2021, the U.S. Intelligence Community's Annual Threat Assessment identified China's efforts to expand its global influence as one of the top threats facing the United States and predicted that cyber operations from China are likely to intensify. This sustained tension, coupled with continued U.S. vulnerabilities in cyberspace, underscores the ongoing need for increased cyber preparedness.

2.4 Timeline

August 30, 1969

The Advanced Research Projects Agency Network (ARPANET), a computer network developed by the U.S. government to ensure that the country maintains telecommunications capability in the event of a nuclear attack, goes online. Originally, ARPANET connects only a few dozen scientists, but it eventually expands to become the global internet.

January 19, 1974

After Chinese People's Liberation Army (PLA) troops occupy parts of the Paracel Islands in the South China Sea, which had until then been held by South Vietnam, Vietnamese troops attempt to retake the islands. Soldiers from both sides are killed in the fighting, but the PLA is ultimately able to repulse the Vietnamese navy.

November 2, 1988 - November 3, 1988

A Cornell University graduate student named Robert Morris releases a program aiming to measure the size of the internet, but a mistaken line of code causes the program to infect and shut down some six thousand computers, approximately 10 percent of computers connected to the internet at that time. The malware is the first to spread widely on the internet. The incident promotes more research into computer security and essentially creates the cybersecurity industry. Morris is also the first hacker prosecuted under the 1986 Computer Fraud and Abuse Act.

May 1999

After U.S. forces bomb the Chinese embassy in Belgrade during a North Atlantic Treaty Organization (NATO) peacekeeping operation, Chinese hackers conduct distributed denial-of-service (DDoS) attacks and deface the websites of federal government agencies, temporarily knocking the White House website offline. The United States maintains that the bombing was an error.

April 1, 2001

A U.S. EP-3E reconnaissance aircraft collides in midair with a Chinese fighter jet seventy miles off the southern coast of China, forcing the damaged U.S. plane to land in China's Hainan province. The U.S. crew is detained for eleven days; the Chinese pilot dies when his jet crashes into the water. In response, Chinese hackers launch a campaign to deface U.S. websites. U.S. hackers respond in kind.

June 2007

Chinese military hackers break into an unclassified Pentagon network that supports the office of the secretary of defense.

July 2008 - August 2008

Russian hackers mount a sustained campaign of cyberattacks that takes down government websites and defaces government and news media websites in Georgia, a former Soviet republic in the Caucasus. Russia subsequently invades the country; cyberattacks continue throughout the conflict.

June 2009 - July 2009

Stuxnet, a virus that targets industrial control systems (computers that operate industrial machinery) and is believed to have been developed by the governments of the United States and Israel, infects computers at Iran's Natanz nuclear enrichment facility. By changing their speed, Stuxnet breaks hundreds of centrifuges that process uranium, crippling Iran's nuclear program.

August 2010

U.S. Department of Defense officials announce a new military strategy for cyberspace, defining cyberspace as "a new domain of warfare" and saying that the United States will pursue tools for the "attack and exploitation of adversary information systems."

May 2011 - July 2011

The PLA reportedly accelerates construction of outposts on the Spratly Islands, a group of small islands and reefs in the South China Sea. China, Malaysia, the Philippines, and Vietnam all claim the islands. The Vietnamese government accuses the PLA of cutting exploration cables towed by a Vietnamese seismic survey ship within Vietnam's exclusive economic zone and announces it will conduct live ammunition drills in the South China Sea.

April 2012 - June 2012

The Philippines deploys its largest warship, purchased from the United States, to Scarborough Shoal, which it contests with China. Philippine troops board eight Chinese fishing vessels and claim the vessels contain illegally caught fish. The Chinese navy deploys two surveillance vessels in response, positioning them between the Philippine ship and the Chinese fishing boats. The two navies remain in a standoff until mid-June; in the interim, the U.S. Navy conducts annual drills nearby with the navy of the Philippines, a U.S. ally.

February 18, 2013

U.S. cybersecurity firm Mandiant releases evidence of an advanced persistent threat (APT), a term for sophisticated cyberattack campaigns likely perpetrated by nation-states, from a PLA unit based in Shanghai. The campaign seeks to steal intellectual property from dozens of U.S. companies across commercial sectors.

May 6, 2013

The U.S. government, for the first time, officially accuses the Chinese military of hacking targets in the United States for both political and commercial espionage.

June 6, 2013

Edward Snowden releases documents showing that the National Security Agency (NSA) has been conducting widespread surveillance of telephone and internet communications of millions of people around the world. Among the documents is evidence that the NSA has been hacking Chinese computers since 2009. A month later, the United States and China begin talks on cybersecurity issues.

May 19, 2014

The U.S. Department of Justice indicts five PLA officers on charges of hacking U.S. companies for commercial gain. In response, the Chinese government withdraws from the bilateral working group on cybersecurity established in July 2013.

February 2015

The Center for Strategic and International Studies, a research organization, releases photographic evidence that the Chinese government is undertaking wide-scale land reclamation activities around reefs in the South China Sea. A few days later, Anthem, the second-largest health insurer in the United States, announces that hackers based in China stole the confidential data of more than eighty million customers. Later in the month, a Russian cybersecurity firm releases evidence that an APT actor, believed to be the NSA, has been hacking thousands of computer networks around the world for nearly two decades.

March 16, 2015

Researchers accuse the Chinese government of hijacking the computers of millions of Chinese netizens to conduct a DDoS attack on websites that help internet users in China circumvent the country's online controls (the so-called Great Firewall). The researchers label the attacking tool the Great Cannon.

June 24, 2015

U.S. officials reveal that hackers stole the personnel records of more than twenty-two million federal employees from the networks of the Office of Personnel Management. Although the government does not formally accuse a foreign government of perpetrating the attack, Director of National Intelligence James Clapper says that China is the "leading suspect" and that "you have to kind of salute the Chinese for what they did."

September 2015

Satellite imagery reveals that China has completed constructing a runway on Fiery Cross Reef large enough to land military aircraft. The reef is part of the Spratly Islands, over which several countries claim sovereignty. Separately, during a bilateral summit in Washington, DC, U.S. President Barack Obama and Chinese President Xi Jinping sign an agreement pledging to not "conduct or knowingly support cyber-enabled theft of intellectual property." They also agree to hold a high-level dialogue on cybercrime starting in December 2015.

October 2015

The guided naval destroyer USS Lassen transits within twelve nautical miles of Subi Reef, one of the artificial islands built by the Chinese government in the Spratly Islands in recent months, demonstrating that the United States does not recognize the artificial islands as Chinese territory.

July 2016

The Permanent Court of Arbitration rules against China and in favor of the Philippines in a case brought by the latter over the sovereignty of the Spratly Islands. The ruling has legal force, but China rejects it, and the court lacks enforcement power. Separately, WikiLeaks releases almost twenty thousand hacked emails from employees of the Democratic National Committee.

August 2016

Photos analyzed by the Center for Strategic and International Studies reportedly reveal Chinese construction of reinforced aircraft hangars on disputed islands, and Vietnam fortifies several of its islands in the South China Sea with mobile rocket launchers.

April 7, 2017

President Donald Trump hosts Chinese President Xi Jinping for a two-day summit. Among other things, the talks result in the establishment of the U.S.-China Comprehensive Dialogue framework. This framework, established to deepen communication and cooperation between the two countries, includes a pillar on law enforcement and cybersecurity.

September 2017

Hackers exploit a vulnerability in popular security software to attack technology companies, several of them American, including Google, Microsoft, and Intel. Security firms suggest that the hack was an act of industrial espionage carried out by an “elite Chinese hacking group” with ties to the Chinese government. Experts see this as yet another instance of increased Chinese cyber intrusions in American companies.

October 6 2017

The United States and China formally reaffirm their 2015 agreement prohibiting cyber espionage for commercial gain. According to FireEye, however, Chinese hacker groups possibly breached the agreement several times in 2016. The chief intelligence strategist for the security firm contends that “the total threat from China didn’t decrease, it just changed shape” after the agreement went into force.

November 16, 2017

In a joint statement, China and the Philippines agree to refrain from using force to resolve the South China Sea conflict. Some analysts see this development as further evidence of improved relations between the two countries under Philippine President Rodrigo Duterte.

November 27, 2017

Federal prosecutors in Pittsburgh indict three Chinese citizens for allegedly launching cyberattacks to steal information from three companies. Reports indicate that the individuals work for a cybersecurity firm that U.S. officials believe is linked to the People’s Liberation Army’s hacking efforts. The hackers are alleged to have targeted Moody’s, an American financial information company; Siemens, a Germany technology firm; and Trimble, an American technology company.

June 2018

Chinese hackers launch a series of attacks on U.S. Navy contractors and universities to steal highly sensitive research and information related to undersea warfare. One major breach involves the theft of secret plans to build a supersonic anti-ship missile for American submarines, according to U.S. officials.

October 2018

The U.S. Department of Justice indicts ten Chinese spies and hackers accused of conspiring to steal sensitive commercial secrets from U.S. and European companies in the aerospace industry. In October 2019, a report from cybersecurity firm CrowdStrike suggests the hacks helped China acquire intellectual property to support the development of its C919 airliner.

February 2020

The U.S. Department of Justice indicts four members of China's People's Liberation Army for hacking U.S. credit reporting agency Equifax in 2017 and stealing the personal information of nearly 150 million Americans.

March 2020

Chinese cybersecurity firm Qihoo 360 accuses the CIA of conducting an eleven-year hacking campaign against Chinese industry targets, scientific research organizations, and government agencies.

December 2020

The cybersecurity firm FireEye first reports a hacking campaign that exploits network management software made by the company Solar Winds. The campaign is attributed to Russian hackers and discovered to have been ongoing since at least February 2020. At least one hundred companies and nine federal agencies report data having been stolen as a result of the hack.

March 2021

Microsoft attributes an attack on email servers to Hafnium, a state-sponsored group operating out of China. The attack affects tens of thousands of victims globally, and the hackers leave behind a "web shell" that allows them continued access to email systems even after Microsoft issues a patch for the exploit.

May 2021

Colonial Pipeline shuts down thousands of miles of pipeline as a result of a ransomware attack attributed to a Russian criminal group, DarkSide. The attack leads to fuel shortages along the eastern seaboard of the United States. Soon after the attack, President Joe Biden releases an executive order designed to improve U.S. cybersecurity.

2.5 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 this 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 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, indicting foreign hackers, and levying sanctions. 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 could 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 could 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 could help small countries build maritime law enforcement and security capacity and in particular improve the Philippines' long-term maritime capabilities. The United States could also expand military exercises with countries 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 could 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 countries to push China harder than they would dare to alone.

2.5 Root Causes

At the heart of this policy decision are territorial issues in the South China Sea and a proliferation of cyberattacks of all types. This combination of policy challenges has three root causes:

1. Thucydides Trap

The Greek historian Thucydides explained that the rise of Athens and the fear its rise created in Sparta made the Peloponnesian War inevitable, and, historically, the rise of new powers has in most cases led to war with the incumbent leading power. Today, the United States is the incumbent and China the principal rising state. Although Presidents Xi and Obama each publicly refuted the idea that conflict is inescapable, analysts on both sides of the Pacific have characterized the current bilateral relationship as one of strategic mistrust. In recent years, the Trump administration's more robust approach to U.S.-China relations, which includes an escalating trade dispute, has introduced significantly more friction in the relationship between the two countries. After decades of steady military modernization, China has new capabilities on the sea and in the air, space, and cyberspace. Chinese forces are much likelier to come into contact with the U.S. military because they are venturing farther into the western Pacific, where the U.S. military has been the dominant force for decades. Beijing often interprets U.S. actions as an effort to contain China and disrupt its rise, and Washington views Chinese behavior as an effort to exert regional dominance and challenge the international order led by the United States.

2. The information and communication revolution

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 sources of wealth. It has created social and cultural networks spanning 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. Countries, terrorists, and criminals could be able to 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.

3. A lack of norms of state behavior in cyberspace

Countries now consider offensive cyber capabilities as essential to their national security. Approximately forty countries have acquired cyberweapons (that is, malware) for use in offensive combat operations, and many more have purchased tools from private cybersecurity firms. Individuals and nonstate groups, instigated by their home governments or operating entirely on their own, can also launch disruptive attacks. The responsibility for a cyberattack can be masked, making it difficult, if not impossible, to determine who should be punished, which in turn makes it harder to deter an attack in the first place. The global and interconnected nature of the internet also means that cyberattacks have the potential to lead to unintended problems far beyond the target.

Countries have yet to figure out how to limit competition in cyberspace. The transparency and verification processes that help limit nuclear competition—which involves physical weapons, materials, and facilities—do not appear to apply to digital weapons. Malware is impossible to count or control. Although acceptance of international law in cyberspace is growing, great uncertainty remains about how it should be applied. Major powers, including the United States and China, have signaled a willingness to discuss the nature of the cyber threat but have been slow to develop a concrete policy framework.