Cyber conflict and geopolitics

by Richard B. Andres

A picture taken on October 17, 2016, shows an employee walking behind a glass wall with machine coding symbols at the headquarters of Internet security giant Kaspersky in Moscow. (KIRILL KUDRYAVTSEV/AFP/GETTY IMAGES)

Across history, the geopolitical fortunes of great powers have often been closely connected with the rise of radical new technologies. In the current era, one of the most significant and controversial questions facing the U.S. is whether new cyber technology is facilitating the rise of Russia and China; more particularly, whether the growing competition in cyberspace is causing a geopolitical pivot that will eventually allow Moscow and Beijing to replace the U.S.-led liberal international order with one more conducive to their autocratic proclivities.

The idea that the U.S.' opponents are acting aggressively in cyberspace is not new. U.S. presidents have regularly pushed back against China's digital predations since at least 2009. Since 2017, the U.S. has significantly upped the ante, condemning Russian and Chinese actions, and using a variety of diplomatic demarches, tariffs and sanctions to back its demands.

Yet there is still a great deal of uncertainty about how serious Russian and Chinese actions are, and about what their behavior portends for future balances of international power. While U.S. security experts generally intuit that *something* important is happening, there is little consensus about what exactly that is or how significant it is compared to the many other threats currently faced by the U.S. and other democra-

The views expressed in this chapter are those of the author and do not reflect official positions of the National Defense University, the Department of Defense or any other U.S. government organization.

RICHARD B. ANDRES *is Professor of National Security Strategy at the U.S. National War College where his work focuses on developing national cyber security strategy. Across his career he has served as an adviser on strategy to the Bush and Obama National Security Councils and other senior leaders and institutions in and out of government. Dr. Andres holds faculty or board positions at the Johns Hopkins School of Advanced International Studies, the Georgetown University Security Studies Program, the American Enterprise Institute, and Pacific Northwest National Labs.*

cies. Officials are aware that Russia is using social media, doxing and various other methods to conduct what they call cyber psychological operations to increase political fear uncertainty and doubt across Europe and the U.S.; and they know that China is carrying out economic espionage and a variety of information operations. But they are unsure about how likely these actions are to undermine the post-World War II (WWII) international order, or if they will facilitate the rise of a new regional or global system in which Russia and China have significantly more say over the course of events.

Connected to this uncertainty is the question of whether the U.S. is a net winner or a net loser as a result of the struggle in cyberspace. The current generation of leaders responsible for formulating U.S. security policy came of age at a time when the U.S. lead in cyberspace was considered incontestable. For many, the idea that opponents might be gaining more than the U.S. from cyber competition is difficult to accept at either an intellectual or emotional level.

Among politically active groups in the U.S., and particularly among business leaders, the problem is equally tricky. In the private sector, there are often powerful incentives to maintain the status quo. The idea that, over a period of years or decades, foreign cyber psychological operations might undermine democracy, or that state-directed, cyber-enabled economic espionage could provide an opponent with an unassailable economic lead, can seem relatively abstract. On the other hand, economic sanctions threatened or enacted by the U.S. against Russia and China to curb specific bad behavior have immediate and tangible effects. On occasion, this dynamic has led Wall Street to oppose government actions that political and security professionals saw as necessary to constrain bad cyber behavior by Russia and China. For instance, in September of 2018, while conceding that the U.S. needs to confront China, Tom Donohue, President of the U.S. Chamber of Commerce argued in an interview with the *Christian Science Monitor* that "The single biggest threat facing the economy right now is the potential for a real trade war."

A serious theoretical problem underlies the lack of consensus on the geopolitical impact of the cyber struggle. Americans today often find it difficult to conceive of a world in which they face serious competition from other major powers. Americans have largely come to view the current world order as permanent, based on the national instruments of power that brought the U.S. to the fore during the Cold War (1947–91) and held it there after that competition ended. Thus, it is probably fair to say that most Americans (who think about this issue at all) tend to believe that so long as the U.S. maintains the world's most powerful military and does what it has always done economically, its ideals will dominate the international system. In fact, this assumption of permanent preeminence has become so strongly ingrained in U.S. thinking that the idea of great power competition and geopolitics has generally fallen out of most U.S. university curriculums. The overall result is that the current generation of leaders is ill-equipped to assess how Russian and Chinese innovations in cyberspace might undermine and eventually usurp the current system.

This lack of imagination is problematic not least because it is not shared by Russian and Chinese thinkers. Strategists in both of those states have regularly and publicly described the ways in which their countries are harnessing cyber technology to overcome the U.S. lead in more traditional instruments of national power. Moreover, Moscow and Beijing have been clear that they do not agree with important aspects of the current U.S.-led system. Should their plans prove successful, it is likely they will alter these systems in ways inimical to U.S. values and interests. Thus, the first step toward assessing how the competition in cyberspace is likely to affect geopolitics is to begin to expand the way Americans think beyond comfortable post-Cold War paradigms. American experts should reflect more generally on the historical connection between radical new technology and geopolitical pivots, and they should take a leaf out of Russia and China's book and apply some imagination to the issues at hand.

Understanding technology-based geopolitical pivots

The idea that new technology can alter geopolitical balances of power has long dominated the thinking of both historians and major power strategists. Writing in the fifth century BC, the Greek historian Herodotus described how Egypt was able to take advantage of new irrigation technology to expand its economic and military might, eventually becoming the most powerful state in the ancient world. Writing more than 2,000 years later, the American naval theorist Alfred Mahan described the role played by maritime technology in the rise of the states on Europe's Atlantic seaboard during the age of sail. A few years later, in a work that foreshadowed World War I (WWI) and WWII, British geographer Halford Mackinder predicted how new railroad technology would facilitate the rise of Europe's land powers at the expense of maritime nations like Britain.

While it is difficult to predict how any new technology might shift international balances of power, both Mackinder's and Mahan's theories provide some clues about what to look for. Mackinder first came to fame in 1904, when he published a paper in *The Geographical Journal* arguing that an emerging technology originally invented and championed by Britain would soon be used by its adversaries to upend its centuries-long position of primacy in world politics. In simplest form, Mackinder's argument was that the economic, military and political primacy of Britain depended on maritime technology. Railroad technology had largely originated there, and Britain appeared to maintain an unassailable technological lead. Yet, Mackinder contended, as continental powers like Germany and Russia developed new railroad networks to gain access to their hitherto inaccessible internal resources, their economies would come to eclipse Britain's. More than this, Mackinder believed that the incentive structure for violence that accompanied rail and continental expansion would alter the way states vied for power. All of this would lead to an international system in which Britain would be poorly equipped to compete. Mackinder's predictions proved accurate. Within a decade, Germany and Russia were battling for supremacy on the continent, and by mid-century, as the Soviet Union completed its rail networks and annexed Central Europe, a single victorious continental power emerged to eclipse Britain.

Mackinder's and Mahan's work provide two general arguments about what is necessary for a new technology to change the geopolitical status quo. The first is that the new technology must be able to significantly change the way geography affects nations' ability to generate wealth and military power. As Mahan described it, in the five centuries preceding the advent of railroads, the diffusion of maritime technology radically improved the ability of states on Europe's Atlantic seaboard to create wealth. During this period, for instance, a sailing ship might circumnavigate the globe in the time it took a laden wagon or army to move a few hundred miles over land. Based on geographical variables such as access to ports and the presence of a population skilled in maritime commerce, states that were able to take advantage of this dynamic had the potential to build their economic and military influence much faster than states that did not. However, as Mackinder noted, when rail technology diffused across Europe, the new technology ended the upper hand enjoyed by maritime powers and provided an unassailable advantage for the economies of large continental powers.

Mahan and Mackinder's arguments further imply that a new technology can interact with geography to change the way that nations compete for security. According to Mahan, maritime technology created a set of incentives that had to be followed for a sea power to achieve primacy. Beyond working to benefit from maritime trade, a global power needed to control that trade by dominating the seas militarily. To control the seas, the state needed to be willing to fund a powerful navy, gain access to global basing and control the world's key maritime chokepoints. While Mahan's notion of control of the sea was assertive, it was not domineering, as maritime mastery depended on free trade and consortiums rather than on the conquest and domination of other states. Thus, the path that maritime technology provided to world power often incentivized nations to compete for military control of the sea, but not necessarily of the territory of other states.

Russian army engineers seen here laying a track bed for a narrow gauge railway during the Russian campaign of March 1916 during World War I. (DAILY MIRROR ARCHIVE/MIRRORPIX/GETTY IMAGES)

Describing the diffusion of rail technology and the rise of continental power, Mackinder envisioned a significantly different set of incentives. He believed that the route to power lay in controlling the resources of Central and Eastern Europe recently opened up by rail. This territory not only offered access to the bulk of the world's industrial capacity, it also provided a secure base that was militarily inaccessible to peripheral powers. He argued that this created a nearly insurmountable security dilemma for the continental powers. Whichever was the first to conquer Central and Eastern Europe would become the master of Eurasia and thus the world. This type of incentive structure would lead inevitably to aggressive competition for control of territory.

Beyond these two characteristics, both Mahan's and Mackinder's work on geopolitics hint at a common irony. In the geopolitical pivot each author describes, the power that did the most to develop the relevant technology—the Hapsburg Empire in the case of maritime technology and the British Empire in the case of rail—eventually lost its primacy when adversaries adopted and adapted the technology for their own purposes. In the current era, the diffusion of cyber technology appears to be following a course with similarities to these geopolitical pivots.

A cyber geopolitical pivot

Like 15th century maritime technology or 19th century rail technology, cyber technology was originally championed by the world's leading state and, over a period of decades, eventually diffused around the globe. Maritime technology accelerated the economic growth of the Atlantic states and rail aided Europe's land powers; the effects of cyber technology are not as straightforward.

In the first place, the term cyber technology is not well defined. In general, it refers to computers and computer networks. This includes telephones, telecommunications networks, and data both in motion and at rest. In and of itself, this infrastructure is important. However, from the perspective of geopolitical power such a definition is incomplete. To truly understand why cyberspace is geopolitically relevant, it is necessary to understand that, over the last three decades, nations have connected virtually everything associated with their economies and national security to computer networks. Thus, the definition needs to expand to include much more than computers and data per se.

In terms of economics, the way wealth is generated and stored has changed in fundamental ways since the beginning of the cyber age. Leading up to the 1980s, around 80% of most U.S. companies' wealth was stored in tangible assets. From a security perspective, this meant that the key to national wealth was control of hard assets like land, natural resources and factories. In the worlds with which Mahan and Mackinder were dealing, the key to maintaining national power was maintaining control of economically productive territory and populations, as well as economic lanes of communication like land and maritime chokepoints. This is no longer true in the cyber age. Today, around 80% of most U.S. companies' wealth is stored in intangible goods, mainly trade secrets and intellectual property. These types of goods are not particularly vulnerable to territorial conquest or conventional seizure of land or maritime lanes of communication. They are, however, extremely vulnerable to certain types of cyber piracy, and their security depends on which actors control the cyber networks on which they are stored and across which they flow. In this sense, cyber technology has probably changed the way that wealth is generated, stored and transported at least as much as maritime and rail technologies did in previous centuries.

Cyber technology has also altered the character of military power. Before the cyber age, military power was generally measured in terms of the number of troops and weapons a nation could maintain. Today, as nations have computerized and networked their weapons, mere numbers have become increasingly irrelevant as indictors of military power. It has not been uncommon in recent wars for computerized and networked militaries, utilizing advanced sensors, communications and precision munitions, to inflict hundreds or even thousands of casualties for every one inflicted when fighting non-networked forces. Yet to achieve these results, modern forces have had to connect their systems to hardware and software that is often vulnerable to cyberattacks.

In an earlier age, the domestic critical infrastructure of strong advanced economies like the U.S. was often made all but invulnerable to attacks by foreign conventional militaries. Today, with most domestic infrastructure connected to computer networks, conventional defenses no longer offer much direct protection; any state with strong offensive cyber capabilities has the potential to do immense damage to a major power's critical infrastructure. Maritime and rail technologies once altered the fundamental requirements of military security for many states. Today, the security once derived from conventional military and geographical advantages is undermined by vulnerabilities inherent in networked domestic infrastructure.

Cyber technology is also altering geopolitical balances of power in more insidious ways. These have less in common with the maritime and rail models described above. In the pre-cyber era, nations generally had a good deal of control over the information their citizens received. In autocratic states, this control generally resided in the government; in democracies, it was located in civic institutions. While nations regularly conducted information operations against their opponents' citizens, these actions were relatively expensive and difficult. In the cyber age, information easily traverses national borders. This makes information operations far easier and cheaper to conduct, and it incentivizes states to attempt to influence the beliefs and behavior of foreign populations.

Yet understanding how states *might* use cyber technology is quite different from knowing how they are actually using it. The following section describes how the U.S., Russia and China have attempted to profit geopolitically from cyber technology over the last three decades, and how the competition in cyberspace has evolved to the benefit and detriment of each power over time.

The United States

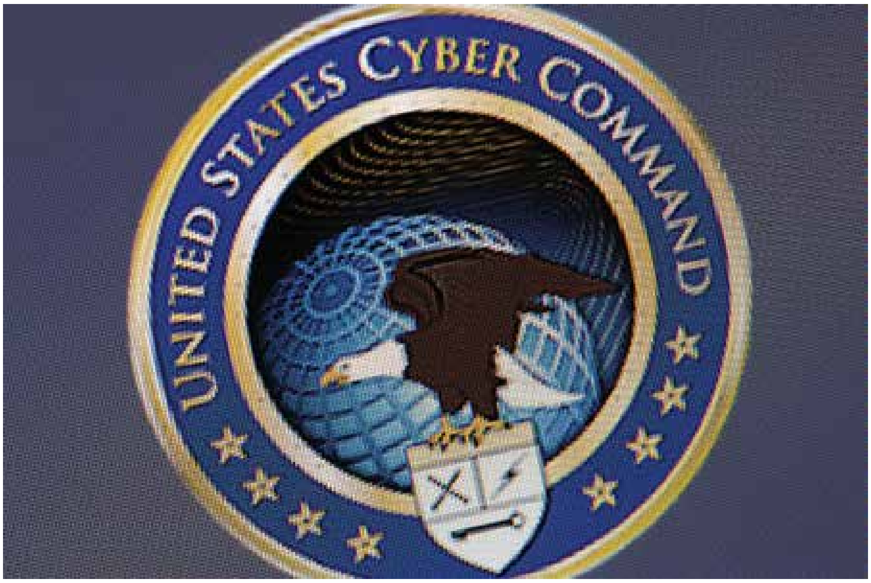
The first power to take advantage of cyberspace for geopolitical gain was the U.S. As the originator of the technology, it had substantial first-mover advantage. As networking morphed from a small Department of Defense-centered project into the global Internet in the 1990s, U.S. intelligence agencies began to use cyberspace for espionage. One of the key lessons learned during this period was that, dollar for dollar, cyber espionage is hundreds-of-thousands or even millions of times more efficient at bulk data collection than traditional forms of spying. By the middle of the 2000s, U.S. intelligence had garnered a reputation in some parts of the world for supernatural clairvoyance.

In 2010, the role of cyber power in international politics changed radically in two ways. The first involved the Stuxnet "worm"—a piece of malware, or malicious software, that multiplied itself and spread between computers, in this case infesting critical infrastructure around the world. The cybersecurity and anti-virus provider Kaspersky Lab attributed Stuxnet to the U.S. government. Until this point, it had been widely assumed that states used malware exclusively for gathering information or, at worst, to sabotage adversaries' computers. Stuxnet turned this assumption on its head: It was designed to destroy hardware attached to a computer network. Specifically, it was designed to spread globally until it eventually infected an air-gapped (completely isolated from external networks) computer network at Iran's nuclear facility at Natanz. At that point, it slowly and stealthily destroyed the centrifuges connected to the network. While Washington did not take credit for the worm, it is widely believed that the U.S. and Israel designed the software with the goal of damaging Iran's nuclear weapons program without crossing a line that could lead to war.

In the same year that Stuxnet became public, the U.S. declared that it was engaged in a global effort to use its cyber capabilities against its autocratic adversaries. In January, on the heels of an announcement by Google that Chinese intelligence had hacked into its computers in order to track down dissidents, Secretary of State Hillary Clinton (2009–13) publicly rebuked Beijing, and delivered a speech on Internet freedom in which she stated that:

"[The U.S. is] also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship. We are providing funds to groups around the world to make sure that those tools get to the people who need them in local languages, and with the training they need to access the Internet safely. The U.S. has been assisting in these efforts for some time, with a focus on implementing these programs as efficiently and effectively as possible. Both the American people and nations that censor the Internet should understand that our government is committed to helping promote Internet freedom."

Clinton's speech, which was representative of the Obama administration's larger goal of spreading democracy, provided the world's autocracies with indisputable evidence that the U.S. was attempting to undermine their systems of government. Not surprisingly, in the wake of the speech, China's Communist Party immediately began to complain of interference in its domestic affairs and greatly increased its spending on cyber based internet policing. (A year later Russian President Vladimir Putin [2000–08, 2012–present] accused Clinton of inciting unrest during the 2011 Russian elections.) When the social media fueled revolutions of Arab Spring began to spread across Northern Africa a few months after Clinton's speech, many observers in both democratic and autocratic nations took it as a sign that the programs Clinton had described were working. While scholars will long debate the actual impact of the U.S. freedom of information operations on the Arab Spring, what is clear is that the speech and the programs it described provided a wakeup call to China and Russia and were instrumental in how Russia chose to adopt and adapt cyber technology over the next few years.



Screen grab of the logo of the U.S. Cyber Command.(ALEX MILAN TRACY/ZUMA PRESS/NEWSCOM)

Taken as a whole, the various uses to which the U.S. put its cyber capabilities were not revolutionary. While they extended and broadened Washington's role as *primus inter pares* in international politics, the U.S.' economic and military strength would almost certainly have accomplished something similar even in the absence of cyber tools. What they did do very well, however, was to provide a new means for countries to connect with each other and demonstrate to Russia and China that cyberspace could be used for geopolitical purposes. Both countries quickly followed the U.S. example but in innovative and revolutionary ways the U.S. had not anticipated.

Russia

Russia began the cyber age at a significant disadvantage. In the wake of the Cold War, Russia had a gross national product that was about the size of the U.S. defense budget. To make up for its lack of resources, in the late 1990s Moscow began to experiment with new ways to use cyberspace. Its first major adaptation was to develop a global network of criminal connections that it could use for economic purposes and as a tool of espionage. These irregular forces both improved Russia's economy, on the margins, and extended the reach of its intelligence agencies. Moscow's second adaptation involved uses of cyber technology against small local rivals: first to paralyze Estonian critical infrastructure during a diplomatic clash in 2007, and later to assist in the invasion of Georgia in 2008. Neither of these innovative uses of cyber technology appears to have done much to change Russia's influence among major powers.

In 2011, however, following Clinton's Internet freedom speech, the Arab Spring and Putin's accusations of U.S. meddling in its election, Russian cyber policy underwent a major change. Before the election, Russian leaders do not appear to have taken cyber information operations very seriously either at home or abroad. During the 2011 election, for instance, Putin appears to have relied chiefly on civilian supporters and criminal groups to disrupt attempts by protesters to organize. After the election, however, Russia's thinking about information underwent sweeping changes, as Putin became convinced that the U.S. had mobilized cyber technology to back protesters. In 2014, Russia's military doctrine was rewritten to include sections addressing information warfare that were absent

Russia's President Vladimir Putin (L) and Russia's First Deputy Defense Minister, Chief of the General Staff of the Russian Armed Forces Valery Gerasimov, attend the main stage of joint Russian and Belarusian military exercises, near Leningrad, September 18, 2017. (MIKHAIL METZEL/TASS/GETTY IMAGES)

from its 2010 military doctrine. While the 2010 doctrine discusses protecting information channels from hacking, the 2014 doctrine describes ways to use information to weaken states by exploiting popular protests and decreasing civilian patriotism and support for the state. Much of the thinking behind this change was expounded in a 2013 article written by Chief of the General Staff of the Russian Armed Forces Valery Gerasimov. In what came to be known as the "Gerasimov Doctrine," the article argues, among other points, that Moscow should adopt and adapt U.S. cyber methods to Russian purposes.

Between 2011 and 2018, Russia experimented with, and ultimately perfected the use of, cyber information operations to influence pro-Western nations. The program began in 2013 with a project led by Kremlin aide Vyacheslav Volodin aimed at the "systematic manipulation of public opinion through social media." Volodin established the Internet Research Agency (IRA), an organization tasked with spreading pro-Kremlin posts on social media and news sites in Russia and abroad. The IRA utilized a number of methods, but the main one involved employing individuals to write and repost stories to social media with the goal of fomenting dissention and undermining the legitimacy of established political institutions. The posters, often referred to as trolls, experimented with a wide variety of methods to achieve their goals.

In 2014, the IRA had some 250 employees. Although the organization's origins are shadowy, its first main foreign target appears to have been the Ukraine and its goal to increase turmoil during Russian operations there. Over time they expanded their operations to Europe and North America. In 2016, U.S. special counsel Robert S. Mueller indicted a group of Russians for interfering in that year's presidential election. The indictment accused the Russians of creating fake Facebook accounts with the goal of manipulating the election. Perhaps most interesting, it accused them of planning and promoting political rallies for Presidential candidates Donald Trump and Hillary Clinton.

Russia's cyber experiments have become increasingly bold and effective. In Europe, Russian operations seem to have played a significant role in increasing anti-U.S., anti-EU and anti-NATO sentiment, as well as support for nationalist movements including: the Basque Nationalist party in northern Spain, the Five Star Movement in Italy, the Vote Leave campaign in the UK, the National Front party in France and the Alternative for Germany party.

Beyond social-psychological manipulation, Russia also uses its cyber capabilities against physical infrastructure. In March 2018, as part of a package of sanctions against Russia, the Department of Homeland Security (DHS) issued an alert warning that Russia was placing malware on U.S. critical infrastructure. The alert shed light on November 2014 testimony by Admiral Michael Rogers, then the commander of U.S. Cyber Command (2014–18), before the House Intelligence Committee: Admiral Rogers stated that China and "probably one or two others" had the ability to flip the switch on the U.S. power grid and other critical infrastructure. The DHS alert also clarified reports from private industry going back to 2012 that implied that most electrical infrastructure around the world was infested with malware, much of it originating in Russia.

The problem of critical infrastructure attack is not well understood by the general public but is taken extremely seriously by the U.S. Department of Defense. Based on their assessment of the severity of the threat, the U.S. Defense Science Board proposed that the U.S. should consider nuclear retaliation as a possible instrument of recourse against this type of cyberattack.

Placing malware on its adversaries' critical infrastructure has the potential to significantly increase Russia's power projection capability and to provide it with diplomatic bargaining capital. Inasmuch as such attacks could be calibrated to affect different levels of damage, they are an inexpensive substitute for long-range conventional arms like aircraft carriers and bombers, which only the U.S. can currently deploy in large numbers. The threat of a Russian cyberattack undermines U.S. deterrence, particularly U.S. extended deterrence commitments to allies. In 2017 testimony to the Senate, former Director of National Intelligence James Clapper (2010–17) explained why the administration of President Barack Obama (2009–17) did not retaliate against Russian cyberattacks in 2016:

"…[W]e'll never be in a position to launch a counter attack…and we're always going to doubt our ability to withstand counter retaliation."

Where Russia appears to have successfully adopted methods to protect itself against cyberattacks, the West has proved highly vulnerable: It has fallen victim to Russian cyber psychological operations, and James Clapper's testimony suggests that it is at risk of critical infrastructure penetration. By adapting and adopting U.S. cyber methods, Russia has done disproportionate political damage. Nonetheless, with a gross domestic product (GDP) one fifteenth the size of the U.S.', it is unlikely that there is anything Russia could do to fundamentally improve its geopolitical fortunes or to catapult it to regional hegemonic status in Europe. While it could be argued that Russia is gaining proportionately from its strategic use of cyberspace, there is little chance that it will be able to use its cyber capability to achieve anything remotely resembling the geopolitical pivots described by Mahan and Mackinder.

China

China appears to have realized the importance of cyberspace in geopolitics as early as 2004. If General Gerasimov is the face of the Russian information doctrine, Major General Li Bingyan is a sort of standard-bearer for China. Writing in 2004, in the context of clear U.S. hostility to the autocratic excesses of China's Communist Party (CCP), rapid U.S. economic expansion, and a string of U.S. military successes in Central Asia and the Middle East, Li argued that China must use information and cyber capabilities to push back against U.S. primacy.

Applying a parable attributed to Chinese leader Mao Zedong (1949–76) about the best way to get a cat to eat a hot pepper, Li argued that China needed to adopt a cyber policy based on deception and reflexive control. As the parable tells it, the best way to get the cat to eat the pepper is not through violent force; rather, one should grind the pepper into powder and place it on the cat's fur. Since a cat cannot help but lick its fur, its instincts will lead it to consume the pepper of its own accord. As it applies to cyber conflict, the notion is that China cannot overcome U.S. technology directly, but can come to dominate the information arena by taking advantage of U.S. laws, instincts and customs, particularly the commitment to freedom of information.

To implement this approach, China began by adopting the cyber espionage tools pioneered by the U.S. and adapting them to its own needs and capabilities. Since the mid-1990s, the U.S. had gained a reputation for using the Internet to bypass geographical boundaries and take information from its adversaries' most protected institutions. In the mid-2000s, China began to replicate these methods. What it lacked in technical know-how, it attempted to make up for in sheer mass and audacity. In 2013, the U.S.-based telecom company Verizon reported that 96% of all state-affiliated cyber espionage attempts against intellectual property (IP) originated in China. In 2014, Federal Bureau of Investigation Director James Comey noted that "There are two kinds of big companies in the U.S. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese." As Admiral Rogers' earlier quote suggests, China also appears to have used the access it developed to infiltrate its adversaries' critical infrastructure.

China adopted the tools of cyber espionage pioneered by the U.S., but it adapted them in one radical way: Where the U.S. had used cyber tools mainly for traditional state-centered espionage, China aimed mainly at commercial targets. Before 2004, China's economic growth had come to depend heavily on commercial espionage and IP theft. By taking advantage of cyber efficiencies, China was able to download millions of times more data than it had previously transmitted via paper and microfilm. In fact, in the mid-2000s, the intake became too much for China's existing espionage institutions to digest. To solve this problem, the CCP developed a series of national plans to manage the influx of digital IP and get it to commercial firms that could convert it to market shares. This involved changing laws, developing bureaucracies and otherwise redesigning parts of China's commercial and civil society.

A wanted poster for five Chinese hackers charged with economic espionage and trade secret theft, released by the Justice Department in Washington, DC, May 19, 2014. The men are accused of being part of a Chinese military unit that has hacked the computers of prominent American companies to steal commercial secrets. (JUSTICE DEPARTMENT/THE NEW YORK TIMES/ REDUX PICTURES)

According to the methods laid out by General Li, however, the focus on commercial IP was only part of the new logic of cyber conflict. Cyber methods depended on a cooperative victim. If IP developing companies fought back, they could severely reduce China's access to their institutions. To reduce the chances of this occurring Li suggested that China should employ "thought control." In practical terms, this means using a combination of modern public relations techniques married with more traditional methods of infiltrating potentially hostile organizations and using economic and sometimes physical intimidation against potentially hostile individuals or organizations. Together, these information steering methods are often referred to both in China and abroad as "Magic Weapons." *The Economist* and *New York Times* have regularly written about these methods, generally with little result. China spends billions on these sorts of information operations every year. More worrying, though, are the more insidious forms of political-psychological operations it conducts abroad.

One of the cleverest methods China employs along these lines involves Hollywood. In the 1990s, political scientists argued that U.S. films were one of the strongest methods of broadcasting U.S. values abroad. Ironically, in the current era, it has become a truism in Hollywood that U.S. films and TV shows cannot make a profit unless they are shown in China. Because CCP censors screen Western media, in effect the CCP has the final say about content involving China in most movies and TV shows that come out of Hollywood. This does not only effect Chinese audiences. Because it is usually prohibitively expensive to film two versions of movies and televisions shows, scripts that are likely to be censored by the CCP are simply rejected. Moreover, because China has cultivated a reputation for doing business with trusted studios, companies often shy away from producing films even for non-Chinese audiences that might hurt their relationship with Chinese censors. The overall effect is that much of what U.S. studios produce is designed to "direct though" in the ways that further China's geopolitical goals.

China's Hollywood connection is only one of many ways the CCP works to reduce Western anxiety about China's policies. Recent studies have shown sophisticated programs to influence Western academia, business and politics. These methods involve holding out promises and threats that demonstrate little tolerance for Western academics or businesses that deviate from the CCP agenda. One particular anecdote is illustrative: Thwarting Chinese cyber espionage became a central goal of the Obama administration beginning in 2009. In 2015, after years of fruitless diplomatic efforts, President Obama invited Chinese President Xi Jinping (2013–present) to a summit in Washington, DC, to discuss Chinese cyber industrial espionage. In the run-up to the meeting, U.S. technology leaders (who had recently snubbed invitations to meet personally with Obama) accepted a public invitation to meet with President Xi. This unequivocal show of support for the Chinese leader undermined President Obama's bargaining leverage. The summit ended in little more than a symbolic promise by Xi to stop cyber commercial espionage. U.S. business leaders, fearful of losing profits in the short term, had enabled Xi's massive commercial espionage program to continue.

Xi Jinping, China's president (L) shakes hands with U.S. President Barack Obama as they depart following a joint news conference in the Rose Garden at the White House in Washington, DC, on September 25, 2015. The U.S. and China announced agreement on broad anti-hacking principles aimed at stopping the theft of corporate trade secrets though Obama pointedly said he has not ruled out invoking sanctions for violators. (PETE MAROVICH/ BLOOMBERG/GETTY IMAGES)

Three years after the Obama-Xi summit, the U.S. tried another tactic to reduce Chinese commercial espionage. In 2017, President Donald Trump's administration (2017–present) began to publicly describe the ways that China was using its cyber capabilities as part of a multipronged effort to improve its economy through commercial espionage. In June 2018, the White House Office of Trade and Manufacturing Policy laid out the administration's perspective in a report entitled *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the U.S. and the World*. The report described an aggressive Chinese campaign with the potential to significantly damage the U.S. economy. Where previous diplomatic disputes with China had often been handled with distinct subtlety, the June report left no doubt as to the high geopolitical stakes involved.

In July 2017, citing unfair trade practices and emphasizing IP theft and illegal technology transfers, the U.S. imposed 25% tariffs on $34 billion-worth of Chinese imports, setting off a tit-for-tat escalation that eventually resulted in what could be described, in absolute terms at least, as the largest trade war in history between the two countries.

As the situation exists today, it is unlikely that U.S. actions will force China to halt its cyber espionage program. The problem is that the CCP is not likely to back down unless the total cost of U.S. tariffs is both economically and politically greater than the sizeable benefits it receives from its cyber espionage program: To a large extent, the CCP's domestic legitimacy is dependent on its record of economic growth; it believes that a sharp decline in this area would be a recipe for civil unrest. Concurrently, the U.S. economy would be likely to take a significant hit if it were to increase tariffs and sanctions to the level required to force Chinese cyber retreat. It is not clear that the American people would be willing to accept such a blow in pursuit of the relatively abstract goal of preventing a geopolitical pivot. Thus, there is a good chance that China will continue to pursue its current course.

With this in mind, it remains difficult to predict whether China's cyber economic espionage campaign will result in a geopolitical pivot. Calculating precisely how much China's economy gains from hacking commercial IP would be no easier than computing how much 18th century Britain's economy gained from its naval dominance, or 20th century Russia and later the Soviet Union gained from railroad technology. Official estimates do, however, provide some clues. In 2015, the Office of the Director of National Intelligence concluded that economic espionage by hacking cost the U.S. economy $400 billion per year. In 2017, the U.S. IP Commission calculated that the "annual cost to the U.S. economy continues to exceed $225 billion in counterfeit goods, pirated software, and theft of trade secrets and could be as high as $600 billion." In 2012, Director of the National Security Agency General Keith Alexander (2005–14) termed cyber commercial espionage "the largest transfer of wealth in history." These figures fail to consider IP taken from non-U.S. sources, which would increase these numbers considerably. In conjunction with China's astonishingly high and sustained economic growth, it is probably safe to assume that cyber commercial espionage has done as much to change the balance of wealth between major powers as did the advent of maritime or rail technology in earlier eras. It is probably also safe to assume that unless the West finds a way to curtail this use of cyber technology, China's economy will continue to grow faster than the economies it is exploiting.

Unlike Russia, China has a GDP comparable to that of the U.S. Given current trends, China's economic power will become much larger than that of the U.S. in coming decades. Accompanied by its domestic political shift toward autocracy and its increasingly assertive military posture, it is probable that China's economic growth foreshadows a geopolitical pivot. To the extent that this growth depends on cyber commercial espionage, it constitutes a cyber geopolitical pivot. Ironically, the cyber infrastructure and methods that paved the way for this shift were developed by the U.S. in the 1990s, and they continue today due to a perverse incentive structure that induces academia, business and politics to reflexively defend a system that is likely to alter the world system in ways these actors will ultimately regret.

THE RUSSIAN TOOLBOX IN THE 2016 ELECTION
YES NO ?
PROPAGANDA, FAKE NEWS, TROLLS, AND BOTS
HACKING AND THEFT OF POLITICAL INFORMATION
TIMED LEAKS OF DAMAGING MATERIAL
ASSASSINATION AND POLITICAL VIOLEN
INVESTMENT CONTROL IN KEY ECONOM
SHADY BUSINESS/FINANCIAL
CORRU

Senator Sheldon Whitehouse questions former Director of National Intelligence James Clapper and former Acting Attorney General Sally Yates during a Senate Judiciary Committee hearing on Russian Interference in the 2016 presidential elections in Washington, DC, on May 8, 2017. (SAMUEL CORUM/ANADOLU AGENCY/GETTY IMAGES)

Conclusions

Yet this version of a geopolitical pivot, based on China's information operations against the West, does not take into account the entire story. China's assertive use of cyberspace is based on a broad set of incentives that rewards states for covertly attacking each other via global computer networks. It originally encouraged the U.S. to spy on its adversaries and eventually to attempt to alter their governments through Internet freedom programs. Currently, it incentivizes Russia to foster nationalism, foment chaos in the West and infiltrate Western critical infrastructure in ways serious enough for U.S. defense leaders to draw parallels with nuclear war. It similarly encourages Chinese programs to embed malware in critical infrastructure and to loot Western companies for their IP.

The first two rounds of the international contest for cyber dominance have already unfolded: In round one, the U.S. government developed the cyber methods that Russia and China went on to adopt and adapt in round two. The game is unlikely to end here. Persistent access to adversaries' networks offers attackers the potential to affect virtually anything attached to a computer. Russia appears to have resolved its vulnerability to cyber psychological penetration, but has built an economic system susceptible to attacks on the computers that control its finances. Currently, China is increasingly using computers to assist in its attempts to control its population. Such a state may be easy pickings for hackers. Despite such potential weaknesses, autocratic states that do not traditionally value freedom of information appear to have an advantage in cyberspace.

It is no more inevitable that cyber technology will lead to a geopolitical pivot on Russian and Chinese terms than that the maritime and rail technologies of past centuries automatically resulted in the world systems described by Mahan and Mackinder. Prophecy is a fraught art. Yet the last two decades suggest that the incentives for low-intensity cyber conflict do exist, and, so far, the guardians of Pax Americana appear to be ceding ground.

discussion questions

1. President Donald Trump announced in 2018 the intent to create a Space Force to protect American interests in space. How will the creation of this military branch affect the U.S. in relation to cyber conflicts? Will it help protect American cybersecurity? Why or why not?

2. In 2011, Russian president Vladimir Putin accused then-Secretary of State Hillary Clinton of sparking conflict during Russian elections that year. How does this relate to the 2016 U.S. presidential election? In what ways has cyber conflict affected elections?

3. How does China and the U.S.'s economic ties affect their relationship with cyber politics? Can the U.S. afford to stop Chinese cyber espionage and face economic consequences?

4. Cyber space is not a tangible object. What are the ways in which geography affects cyber security and conflicts? How are geopolitics and cyber conflict related?

5. Cyber conflict is arguably the newest form of military and global conflict. How do you think the advancement of technology will affect global conflicts?

6. Cyber hacking has implicated both national and civilian security, with both government organizations and companies like Google reporting having been hacked. How will the potentially personal nature of cyber espionage affect individuals? How do individuals and/or companies fit into global cyber conflicts?

suggested readings

Buchanan, Ben. **The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations**. 282 pp. Oxford, UK: Oxford University Press, 2017. This book shows not only that the security dilemma applies to cyber operations, but also that the particular characteristics of the digital domain mean that the effects are deeply pronounced.

Chertoff, Michael. **Exploding Data: Reclaiming Our Cyber Security in the Digital Age**. 288 pp. New York, NY: Atlantic Monthly Press, 2018. Chertoff explains the complex legalities surrounding issues of data collection and dissemination today, and charts a path that balances the needs of government, business and individuals alike.

Futter, Andrew. **Hacking the Bomb: Cyber Threats and Nuclear Weapons**. 212 pp. Washington. DC: Georgetown University Press, 2018. A *c*omprehensive assessment of this little-understood strategic development, this book explains how myriad new cyber challenges will affect the way that the world thinks about and manages the ultimate weapon.

Kaplan, Fred. **Dark Territory: The Secret History of Cyber War**. 352 pp. New York, NY: Simon & Schuster, 2017. The story of computer scientists and the NSA, Pentagon, and White House policymakers who invent and employ cyber wars—where every country can be a major power player and every hacker a mass destroyer.

Scharre, Paul. **Army of None: Autonomous Weapons and the Future of War**. 448 pp. New York, NY: W.W. Norton & Company, 2018. The author uses military history, global policy and cutting-edge science to argue that we must embrace technology where it can make war more precise and humane, but without surrendering human judgment.

Segal, Adam. **The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age**. 320 pp. New York, NY: PublicAffairs Publishing, 2015. A description of how the internet has ushered in a new era of geopolitical maneuvering that also reveals the terrifying implications for our economic livelihood, security and personal identity.

Singer. P.W and Brooking, Emerson T. **LikeWar: The Weaponization of Social Media**. 416 pp. Boston, MA: Eamon Dolan/Houghton Mifflin Harcourt, 2018. Two defense experts explore the collision of war, politics and social media, where the most important battles are now only a click away.

Don't forget: Ballots start on page 103!

To access web links to these readings, as well as links to additional, shorter readings and suggested web sites,

GO TO www.greatdecisions.org

and click on the topic under Resources, on the right-hand side of the page.