SEPTEMBER 2018

Cognitive Effect and State Conflict in Cyberspace

James A. Lewis

Information technology has reshaped international conflict. The 1990s vision that the end of the Cold War was a triumph for market democracy has proven to be an illusion. Several powerful trends, including the reaction to U.S. supremacy, the fraying of the international order created after 1945, and the political effect of information technology are reshaping international security. There is a broad discontent with the international status quo among new and resurgent powers, and competition and conflict among great powers has been reshaped by information technologies. The nexus of strategic competition is not jihad or defending some imaginary global commons, but over how the world will be ordered and who will order it.

The reaction to globalism and the spread of Western and Americanized culture have led to resurgent nationalism, as societies seek to protect their own values, accompanied by a general discontent with Western values on governance and individual rights that were once thought to embody progress. This is the antithesis of the "one world, no borders" approach of internet visionaries. The reemphasis of sovereignty and the right of a state to govern itself without external interference—and the internet is seen by many as external interference—sharpens conflict.

Authoritarian regimes use nationalism to defend against Western ideals of democracy and individual rights. They see it as the antidote to the rule of (Western) law. Some non-Western states assert that liberal ideals are not universal and are inappropriate for developing or non-Western countries. If the Cold War was a bipolar struggle between two competing systems of governance, this new conflict is multipolar and a struggle against the governance system—market democracy—that emerged as dominant after 1989.

Four countries—Russia, China, Iran, and North Korea—are in conflict with the United States, but this conflict has taken new forms that caught the superpower by surprise. It is not conventional warfare. With the advent of nuclear weapons, major powers have sought to avoid direct military confrontation. Wars between big, heavily-armed states are expensive and risky. Our opponents have not renounced the use of force or coercion, but they are more nimble in its use and try to avoid open warfare with the United States. Cyberspace has become the preferred battleground. Opponent actions inhabit a "grey area," that is neither

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

peace nor war, where the United States and its allies, unable to use military force in response, have often been stymied in designing an effective response.

States exploit the internet for coercive purposes. Its attributes lend themselves easily to coercion, including relative anonymity, a degree of deniability, the powerful cognitive effects information technologies can produce, and its global reach. While cyberattacks can be used to produce effects similar to kinetic weapons, the intangible effects are more important. The manipulation of information and decisionmaking will add complexity to any conflict, provide a source of military advantage, and challenge our conventional, kinetic-oriented strategies.

To be fair, many opponent actions were defensive, started in response to U.S. unthinking efforts to promote market democracy after the Cold War. The internet brought American ideas and expectations to previously insulated nations. Opponents wove a narrative of hostile U.S. intent aimed at regime change and hastened by NGOs working in their own capitals, social media, and a general domination of what Russians call the "information space" through media and internet outlets. What is interesting is that these defensive efforts have moved to the offense, intended to erode U.S. power and disrupt alliances.

Too much of the discussion of "cyber's" role in conflict is shaped by the precedent of nuclear war. Nuclear war threatened catastrophe. Catastrophic cyberattack is, however, unlikely. A major cyberattack is unlikely to produce a crippling blow and could enrage a nuclear-armed opponent. This risk is not worth the result. Cyber operations provide a new way to achieve military and perhaps strategic advantage, but this will not come from some virtual equivalent of nuclear catastrophe or the strategic bombing against industry seen in World War II. Rather, cyber effects will be produced by the manipulation of software, data, knowledge, and opinion. The objective is not kinetic but cognitive effect, the manipulation of information to change thoughts and behaviors. In essence, the strategic goal is to affect morale, cohesion, political stability, and, ultimately, diminish the opponent's will to resist. Operations provide the ability to manipulate information and opinion in ways that have a coercive or disruptive effect, without the risk of open warfare and staying below the threshold of the "use of force" to reduce the risk of armed conflict and escalation.

One benefit of cyber operations is that coercive actions can be taken while minimizing the risk of escalation. In contemplating the use of cyber operations, one factor that weighs upon all opponents is the immense capacity of the United States to inflict punishment, and judging from their behavior, Russia, China Iran, and North Korea have strategies to minimize or avoid the risk of retaliation while still using coercion and to achieve their ends. They weigh the benefits from cyber operations against the risk of escalation and retaliation. We will see increased use by our opponents of coercive acts that fall below the implicit thresholds for the use of force or armed attack.

The Knowledge Revolution and Politics

The internet is transforming society, business and politics as people respond to new opportunities online and change their behavior accordingly. A precedent may come from Gutenberg and movable type. Cheap printing first changed how people thought, and then how they acted. They could acquire knowledge at a lower cost and from a much broader array of sources. This gave them new (and sometimes competing) concepts and narratives, and the new ideas eroded certainty in institutions and authority.

The internet accelerates larger political trends that are redefining the role of the state, the efficacy of liberal democracy, and the authority of the enlightenment values that emphasize the primacy of the individual. These values face powerful ideological challenges from authoritarian regimes at a time when many citizens of Western nations are themselves consumed with doubt. The Western ideal of "progress" and perfectibility are questioned in many regions. New technologies provide an ideal vehicle for this questioning by both domestic audiences and foreign opponents. The effect is to undermine the dominant political narrative of market democracy, a narrative that is already badly tattered by its own shortcomings and as a result of sustained efforts by authoritarian regimes to weaken it.

All countries face political challenge from the internet. Democracies are not immune and face immediate problems, but in the long term, information technology poses the greatest challenge to authoritarian regimes. Information technologies create an existential threat for authoritarian regimes that they are hard pressed to manage. Authoritarian regimes, with their brittle relationship with their own citizens, have reacted by trying to suppress this political effect by restricting access to information, providing counternarratives for both domestic and foreign consumption, and by creating ubiquitous surveillance regimes in a powerful effort to maintain control.

The internet provides new ways for individuals to attach their loyalties and to identify with groups. It disconnects public discussion from physical location and increases the likelihood that community will be defined as those who think like us rather than those with whom we share a space. Before the internet, individuals with extreme views may have been isolated in their community. Now they can go online and find their beliefs reinforced when they find that those beliefs are shared by thousands of others.[1]

The internet is democratizing, if by this we mean greater participation and not an endorsement of democratic political values. Extremist groups who reject liberal values are among the beneficiaries of the "democratization" of knowledge and communication. Over the long term—perhaps decades—greater access to information and greater participation may expand liberal democracy, but the immediate political effect of the internet has been to energize extremist views and increase the numbers of individuals who hold them.

The effect on the mediation of content is most pronounced, with a decentralized media open to millions of contributors displacing the editors and fact checkers of the past. In the 1960s, Daniel Moynihan said that everyone was entitled to their own opinions but not to their own facts. The internet allows people to have their own facts. Social media amplifies this trend. Facebook has become the primary source of news for most Americans, but its structure of "likes" and "friends" means that information presented on it can be culled and shaped to fit group preferences.

Information that runs counter to preferred beliefs is often excluded. Russia, Iran, and China fear the effect of social media on their own societies, but the Russians have been astute in using it to shape western views, while the Chinese use it to impose a conformity in discussion and opinion in their own population that they are now trying to extend to other countries (Australia being the most salient example).

Cyber erodes existing authority and legitimacy by changing citizen expectations and creating competing narratives. Russia has been quick to seize the opportunities that these broad changes present for attack. To defend themselves from the Western informational "onslaught," Russia China, Iran, and North Korea work to create a powerful counternarrative of heroic nationalism, unrelenting Western hostility, and U.S. hypocrisy, using both their domination of national media and censorship efforts to deny their citizens access to potentially disruptive information from the West.

Antipathy to the unipolar moment and a desire to undo the U.S.-centric international structure and attain regional dominance, has led our competitors to develop strategies, tactics, and technologies that can frustrate American power. Their informational goal is to challenge the prevailing Western narrative, to

[1] An early discussion of the effect of the internet on behavior is found in John Suler's "The Psychology of Cyberspace," 2004, http://truecenterpublishing.com/psycyber/psycyber.html.

persuade first their domestic audiences of the successes of their regimes while highlighting American failings.

The first “knowledge revolution” created by the printing press brought centuries of political turmoil. Digital technologies have the same effect, but at a faster pace and with broader consequences. The internet has changed the requirements for legitimacy and assent. For a government to be perceived by its citizens as legitimate requires more than the mechanisms of representative democracy. Representative democracy as currently constructed does not meet the expectations the internet has created among citizens for access to information and direct involvement in decisionmaking. The same pressures that push businesses to adopt flatter, less hierarchical organizations also press on governance. Policy and law will need to evolve to take into account citizen expectations if democratic governments are to rebuild legitimacy. What that new mechanism for democratic governance and legitimacy will be is yet unclear, but it will require greater transparency and direct citizen participation.

The Arab Spring Scenario

When certain conditions are present—discontent and unpopular authoritarianism—information technology and the internet provide a tool for coalescing discontent into action when there is a triggering incident and charismatic opposition leaders. China, Russia, and Iran fear this “Arab Spring” scenario. Then-Russian Prime Minister Medvedev’s claim that the revolts in the Arab world were instigated by Western “outside forces” who were also conspiring to topple the Russian government reflects a common fear among nondemocratic regimes. Medvedev said, “Let's face the truth. They have been preparing such a scenario for us, and now they will try even harder to implement it."[2]

Information is a threat to authoritarian regimes since they lack democratic mechanisms for accommodating dissent and pressures for political change. This has led them to develop countering efforts in a reaction to what Russia, China, and others would call Western information hegemony. Resurgent nationalism as a defense of authoritarianism has only mixed appeal and creates unpredictable political dynamics in authoritarian states. Chinese leaders, in particular, fear that nationalist sentiment it uses to retain popular support could escape their control.

Russia and China use a broad spectrum of media—print, television, film, and the internet—to promote an alternative narrative and to promote a nationalist hostility to the United States and the West. Al Jazeera’s English language channel, created in 2006, says it has “challenged established narrative and gave global audience an alternative voice.”[3] Sputnik, Russia Today (RT), and China’s *Global Times* are used by Russian and Chinese states for similar purposes.

Russian and Chinese discomfort with the dominance of western media (such as BBC or CNN) and their power in creating a global narrative led these nations to create alternatives. Russia and China created competitors—RT (with Spanish and Arabic channels) was created in 2005 and provides a strong anti-American and pro-Russian spin on the news. RT exploits Google rankings to have its stories appear at the top of search results.[4] Putin called RT’s parent entity, Novostni, an organization of strategic importance for Russia.

[2] Nabi Abdullaev, “Kremlin Sees Peril in Arabl Unrest,” *The Moscow Times*, February 24, 2011, http://www.themoscowtimes.com/news/article/kremlin-sees-peril-in-arab-unrest/431523.html.

[3] Al Jazeera, “Who we are,” http://www.aljazeera.com/aboutus/.

[4] Kaveh Waddell, “Kremin-Sponspored News Does Really Well on Google,” *The Atlantic*, January 25, 2017, https://www.theatlantic.com/technology/archive/2017/01/kremlin-sponsored-news-does-really-well-on-google/514304/. In 2011, Secretary of State Hillary Clinton said that the United States was "losing the information war" abroad to foreign channels like RT, Al Jazeera and China Central Television.

China has several state media outlets intended to challenge information hegemony. *Global Times* was repurposed in 2009 to provide English language version to promote a more positive view of China, complete with its sometimes shrill, anti-American commentary, but similar views can be found in the Chinese and foreign language versions (other than English) of official Chinese media outlets. CCTV (China Central Television) created foreign language broadcasts in 1996 (now offering eight major languages) in an explicit effort to create a more positive narrative of events in China. State-supported Chinese actors have purchased media outlets, such as the *South China Morning Post,* and have begun to reshape reporting and editorial policies along these lines. Executives of Alibaba, the Chinese acquirer, said their goal was to "improve China's image and offer an alternative to what it calls the biased lens of Western news outlets."[5]

The effect of these Chinese acquisitions has been to engender a degree of self-censorship among Western firms in order not to alienate Beijing or lose market access. How effective they have been in reshaping foreign views of China is another matter. Similarly, the creation of Confucius Institutes, a somewhat ham-handed effort at generating soft power in the United States (where most of the Institutes are located) has also had mixed results, attracting criticism from a range of sources without noticeable improvement in American views of China.[6] China's problem remains the same as it was in 1926 when a leading Chinese dissident and author, Lu Xun, wrote, "Lies written in ink can never disguise facts written in blood."

Both China and Russia use internet trolls to shape social media in ways favorable to their regimes and damaging to the United States and other opponents. China's focus is largely inward, on controlling their own population, while Russian trolls seek to influence both foreign and domestic audiences. The Russians have been skillful in exploiting Western social media and have successfully automated trolling though the use of "chatbots," computer programs that act as participants in online discussion who amplify and extend the reach of propaganda. Weak governance and commercial indifference gave these chatbots free rein before 2017. Both countries take advantage of democratic guarantees for freedom of expression to maximize access to Western audiences, to include taking full-page ads in leading newspapers or even complete pull-out sections, actions that would have been unthinkable in the Cold War.

Other opponents share the dislike of Western global media dominance, but their efforts are focused on their domestic audiences. Iran's control of the media (television remains an influential source of news for most Iranians outside of major cities) and North Korea's attempts to block access to any source of alternative information are inward focused. Their primary goal is to control their own populations rather than persuade foreign audiences.

Efforts by China and others to isolate their national networks (and, in China, build national industries to produce indigenous technologies) share a fundamental weakness. All of these countries (even North Korea) want some connection to the outside world, if only for business purposes. These connections offer an avenue for their populations to access disruptive information. Similarly, while internet connections provide the most common avenue for access to "unapproved" information, it is not the only avenue, as tourism, entertainment smuggled CDs, and education abroad all undercut the state narrative. The immediate political effect may be small, but it is gradual, corrosive to authoritarian rule, and unsettling to authoritarian regimes.

[5] David Barboza, "Alibaba Buying South China Morning Post, Aiming to Influence Media," December 11, 2015, https://www.nytimes.com/2015/12/12/business/dealbook/alibaba-scmp-south-china-morning-post.html.

[6] Elizabeth Redden, "New Scrutiny for Confucius Institutes," *Inside Higher Ed*, April 26, 2017, https://www.insidehighered.com/news/2017/04/26/report-confucius-institutes-finds-no-smoking-guns-enough-concerns-recommend-closure; Richard Wike, "6 facts about how Americans and Chinese see each other," March 30, 2016, https://www.nas.org/projects/confucius_institutes; http://www.pewresearch.org/fact-tank/2016/03/30/6-facts-about-how-americans-and-chinese-see-each-other/.

Opponent Strategies

China, Russia, Iran, and (to a lesser extent) North Korea, have well-developed military cyber capabilities. In conflicts with them, we should expect to see cyber operations combined with electronic warfare, antisatellite attacks, informational campaigns and other unconventional tactics and weapons. The intent will be to degrade the American "informational advantage" in warfare by attacking communications and ISR assets and capabilities, to slow and damage American decisionmaking and operations, and to create political uncertainty, turmoil, and dissent.

The trajectory of Russian policy over the last 10 years has been to move from being on the defensive in the face of the challenges created by information technology, something the Russians believe was an intentional Western plot to undermine the Putin regime, to being on the offensive. The Russians adopted traditional disinformation techniques to the new technologies and honed their skills by first using trolls, fake news, and damaging leaks again domestic opponents in the first years of Putin's rule. Influenced by both traditional Russian espionage techniques and by new military doctrines, Russia has used the internet as a weapon against the West.

Russia has worked successfully to find tools and tactics that compensate for its weaknesses. Its doctrine seeks to weaken opponents, in what the Russians see as a battle for the "information space," using RT, hundreds of trolls to plant pro-Russian messages in the comment section of western media outlets, "chatbots" to flood social media with hostile comments, and, of course, political damaging leaks purloined emails through various front organizations, including WikiLeaks (along with bribery, hacking, and threats), to reshape western opinion. New Generation Warfare will be dominated by information and psychological actions that seek to depress the opponent's armed forces personnel and population morally and psychologically, and used in the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory.

Russian strategists call information a weapon and uses it against the United States and its allies. Information is not a weapon in any sense recognized by international law, but it can be used to coerce, threaten, and manipulate. Russia's 2014 Military Doctrine calls for "exerting simultaneous pressure on the enemy throughout the enemy's territory in the global information space. . ." Some Russian documents call this "pre-conflict opinion shaping." In the short term, these influence efforts create political turmoil and discord. Russia will take advantage of both the travails of Western liberal democracy and the internet's centripetal impulses towards extremism to undermine democratic governance. Although Russian efforts are clever, they would be far less effective absent these larger political and technological trends.

The Russians know that the Western commitment to free speech makes it difficult to block their disinformation campaign—no one in America or other democracies wants the government to censor the internet (this isn't a problem for Russia, China, Iran, or North Korea, which have no compunction about censoring). Russia has had long practice with disinformation—some of the tricks they used in the 2016 U.S. election date back to the Czars. Neither the United States nor its allies knew how to defend against or respond to this kind of coercive effort.

The Russian goal is cognitive effect, to "achieve political objectives without the utilization of military force." Valeri Gerasimov, chief of the Russian Armed Forces' General Staff, has said that "the 'rules of war' themselves have changed significantly, nonmilitary options have come to play a greater role in achieving political and strategic goals and, in some situations, are greatly superior to the power of weapons."[7] Russia has used its long experience, dating back to the nineteenth century, in what we would now call information operations and which Russians refer to as "reflexive control."[8] Operations to produce cognitive effect and shape the thinking of opponents and neutrals are a central element of Russian military doctrine and New Generation Warfare.

Russia's efforts are not the primary cause of damage to the western institutions and legitimacy. These are self-inflicted, the result of growing inequalities and a general discontent with the pace and direction of social change. Russia exploits and amplifies existing trends, building on the long record of success shown by its intelligence services in creating compelling misinformation—from the Protocols of the Elders of Zion to the canard that U.S. military laboratories created AIDS ("Operation Infektion"). George Kennan's 1946 Long Telegram warned of Soviet efforts to increase disunity, disrupt self-confidence and create unrest in Western nations, and just as Moscow attempted to use "Democratic Progressive" elements in the Cold War, the Russians today look to ultra-right-wing nationalist groups as potential allies and agents of influence.[9] What has changed is the speed and scope of dissemination, the power of new information tools such as leaks and misinformation, and the ease of access to susceptible population.[10]

China's efforts are focused primarily on its own population and Chinese emigrants. Chinese propaganda has been most effective in persuading the world of its inevitable economic ascendancy and in exposing the shortcomings of U.S. policy, but it has not succeeded persuading others that Chinese culture under party rule is attractive. China endorsed the pursuit of "soft power" ten years ago when Hu Jintao called for making "socialist ideology more attractive and cohesive." This will be a difficult objective for China to achieve. Party officials have talked about the imminent return of China to the summit of global soft power as it becomes a "powerhouse of discourse" to match its economic might, [11] but this aspiration is undercut by China's harsh dealings with its neighbors, its domestic repression, and the inherent contradictions of its political system.

Chinese doctrine for the military use of cyber operations is more conventional than Russia's. It focuses on disrupting weapons performance and command functions. Press reports allege that since 2001, more than two dozen major U.S. systems have been hacked, including aircraft, air and missile defense systems, and nuclear weapons. China has undertaken cyber operations to gain access to U.S. weapons systems to understand their operational limits, copy them, and to prepare to interfere with their operations in combat.

Iran and North Korea use cyber actions for coercive effect against U.S. banks or entertainment companies like Sony or the Sands Casino that they want to punish, but their goal is political coercion, not destruction, and the intent may be as much to show their own populations and themselves that the eagle's tail can be twisted with impunity.

[7] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA Analysis & Solutions* (September 16), www.dtic.mil/get-tr-doc/pdf?AD=AD1019062; *Nicholas Fedyk, "Russian 'New Generation' Warfare: Theory, Practice, and Lessons for U.S. Strategists," Small Wars Journal,* http://smallwarsjournal.com/jrnl/art/russian-%E2%80%9Cnew-generation%E2%80%9D-warfare-theory-practice-and-lessons-for-us-strategists.

[8] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256, https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

[9] George Kennan to George Marshall, telegram, February 22, 1946, lhttps://www.trumanlibrary.org/whistlestop/study_collections/coldwar/documents/pdf/6-6.pdf.

[10] Thomas Bohardt, "Operation INFEKTION: Soviet Blog Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence*, Vol. 53, No. 4 (December 2009), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf.

[11] http://chinamediaproject.org/2017/06/24/china-rhetorical-giant-move/

It is worth noting that none of these countries talk about "death by 1000 cuts" or attacking critical infrastructure to produce a "cyber Pearl Harbor." While these ideas (along with the notion of non-state actor attacks on critical infrastructure) are staples of the cybersecurity discussion in the United States, there is no evidence to support them. The public discussion does not reflect the reality of cyber conflict.

An initial assessment is that Russian, Chinese, and perhaps Iranian efforts have been more effective with their own populations, and the Russian counternarrative (and accompanying active measures) have had success in damaging the United States and in unsettling Western democratic processes. However, neither Russia nor China (even with all its wealth, Confucius Institutes, and expatriate groups) has been able to devise an attractive alternative to liberal democracy. Putin's narrative of a rational, nationalist Russia appeals to Slavic populations and far-right fringe groups outside of Russia, but its efforts to woo foreign audiences are undercut by its repressive actions, corruption, and its hostile rhetoric. China's adulatory descriptions of Xi Jinping are unpersuasive to non-Chinese audiences. Both countries struggle unsuccessfully with widely held negative impressions among foreign populations.

The Russian and Chinese message of restraining the United States, replacing the post-1945 world order, and reemphasizing the role of sovereignty is appealing to many nations in the G77 and the Nonaligned Movement, but Russia and China have not been able to turn this appeal into meaningful support for alternative institutions. The idea of the BRICS, a consortium of newly powerful nations outside the transatlantic ambit, is a clever recognition of the changing balance of power, but there is a fundamental fracture among the BRIC nations. India and Brazil have very different attitudes to freedom of expression than Russia and China.

The 2012 World Conference on International Communications saw Russian proposals to redo internet governance gain support from a majority of nations, but this may have reflected the bankruptcy of Western thinking, with its increasingly ineffective defense of the status quo and its emphasis on keeping the internet "open and free." In contrast, Russia found itself isolated at the 2014 NetMundial conference, where its overt political agenda attracted support from only Cuba and (perhaps by mistake) India. A mixture of coercion and monetary inducements are Russia and China's most effective tools for influence.

Unsurprisingly, this assessment of the appeal of the authoritarian alternative has regional variations. Respondents in the Middle East and in some Latin American countries have largely unfavorable views of the United States, while Europe and Asia (outside of China) have (or had) largely favorable views—something that has changed markedly since January 2017.[12] In contrast, two-thirds of respondents in a global survey had unfavorable impressions of Russia, suggesting that the efforts of RT and others have had at best, limited success.[13]

A New Kind of Conflict

It was a mistake to assume that the end of the Cold War meant the triumph of market democracies and the end of conflict and competition among states. The United States finds itself now in a world where its soft power is diminished and its hard power less useful. Emerging powers see themselves as challenging the United States for economic power, international influence, and regional leadership. Some have moved beyond challenge to conflict. In this environment, our opponents will exploit the opportunities created by information technology for damaging the United States and advancing their national interests.

[12] Janell Fetterolf, Jacob Poushter, Bruce Stokes, and Richard Wike, "U.S. Image Suffers as Publics Around World Question Trump's Leadership," *Pew Research Center*, June 26, 2017, http://www.pewglobal.org/2017/06/26/u-s-image-suffers-as-publics-around-world-question-trumps-leadership/.

[13] Margaret Vice, "Publics Worldwide Unfavorable Toward Putin, Russia," *Pew Research Center*, August 16, 2017, http://www.pewglobal.org/2017/08/16/publics-worldwide-unfavorable-toward-putin-russia/.

This is a new kind of conflict whose core is information and the cognitive effect it produces. While the contest to create cognitive effect should favor America and the West, gaining the advantage requires rethinking of ideas, strategies, and narratives. The intellectual principles of American policy—democratic governance and the rule of law—remain strong but need a new articulation if they are to remain persuasive. America's soft power came from compelling ideas, but these ideas have been undercut by waterboarding, Edward Snowden's revelations, and almost two decades of misadventure in the Middle East. Foreign perceptions of U.S. actions in the last 15 years are now much less benign. The 2003 invasion of Iraq (without the blessing of the UN Security Council, a crucial point for many countries that see the UN as a check on the unbridled power of larger countries) appears to have soured foreign views of the United States that an affinity for U.S. popular culture will not easily erase.

We are in a post-1945 world, and this has broad implications for policymaking. Before 1945, governments played a more narrowly defined role both domestically and internationally. Some nations would prefer to return to this traditional definition of sovereignty, where universal rights were less important. The Western model of governance, based on representative, parliamentary democracy, and the enlightenment norms associated with it, no longer ensure the assent of the governed.

The governmental and multilateral approaches developed in the West in response to the global crises of the 1930s—multilateral institutions and rules, and the macroeconomic, managerial state—are no longer adequate (if unreformed) to meet the expectations of citizens that have been reshaped in good measure by information technology and the internet. However, the alternatives to the post-1945 order—untrammeled authoritarian sovereigns or nebulous multi-stakeholder governance—prove even less attractive. Until some new model of governance can accommodate information technologies and their political effect, cyberspace will remain an arena our opponents are only too willing to exploit.

James Andrew Lewis is a senior vice president at the Center for Strategic and International Studies in Washington, D.C.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).