OCTOBER 2020

Sovereignty and the Evolution of Internet Ideology

By James A. Lewis

The **architecture** of the internet is changing as the political concepts that underpin it also change. While the term "ideology" can have negative connotations, in this case it is neutral, referring to the framework of concepts and beliefs that guides decisionmaking. The ideology undergirding the internet has been changing for some time in the direction of greater sovereign control of networks and network activities. This has not come without tensions, but the real risk from expanding sovereignty is not many separate internets but a fragmentation of governance, where the underlying protocols would still support global connectivity, but connectivity overlaid with many uncoordinated and often dissonant rules for data, privacy, and security.

The internet was commercialized soon after the end of the Cold War, when there seemed to be an emerging global consensus that governance would follow the norms of market democracies—the role of government would shrink in a world where the antiquated "**weary giants of flesh and steel**" were unnecessary. It is easy to mock these views, but not too long ago, they were very powerful, part of a larger millennial utopianism that possessed many technocrats and some analysts of foreign policy. Increased international tension, a resurgence of nationalism, and failures to deliver security and privacy have undermined this original ideology.

An evolution in internet ideology was inevitable as the number of users and uses expanded and as its importance as an infrastructure increased immensely. The internet was an American creation, and American values of openness and free speech (shared by many, but not all countries) shaped the internet's technology and governance, often in ways that worked against sovereign control. The issue before us is not how to preserve an illusory commons but how to shape state action intended to serve national interests, recognizing that the interests of all nations do not necessarily coincide, in ways that minimize damage to global connectivity.

What Drives Balkanization

Advocates of the old approach call the assertion of sovereign control "balkanization," but this fails to recognize the concerns that drive nations' actions. The shortcomings in the old approach for privacy and security impel governments to play a greater role to protect their citizens. The internet erodes privacy, security is noticeably lacking, and tech giants stalk the earth with apparent disregard for governments. **Concerns** over possible anti-competitive behavior by a few large companies that dominate the online market reinforce the trend. There is global discomfort with the oversized role of American firms. There is an irony in this, since the people who object to U.S. tech dominance often rely on the services American firms provide. But as concerns over privacy, security, and the erosion of national sovereignty increase, the effect is to change the politics of the internet and reshape its architecture.

The steady extension of sovereign control into cyberspace occurs as nations seek to protect their citizens and find that the laissez-faire approach developed in the 1990s is too weak to do this. This hands-off approach was appropriate at the onset of the commercialization of the internet to shelter the fledging industry and accelerate its growth. Indeed, a regulation-heavy ideology might well have throttled development, and overregulation still poses the risk of slowing growth. But as the internet turned into the most important and most profitable sector of economic activity, the laissez-faire approach developed three decades ago was found wanting.

The internet's now-global population has different values and different expectations regarding the role of government. In 2000, there was no Facebook or other social media, and Google was a tiny startup. By 2010, the internet had become the central global infrastructure for commerce, finance, and security. It creates new and powerful social forces that challenge political stability. In response, states began to assert control.

There is an understandable and reasonable fear that moving from the original ideology and governance structure will damage the economic potential of the internet. A case can be made that regulation, the chief tool for extending sovereign control, slows growth and innovation. Europe missed the tech boom, and while there are many reasons for this, overregulation is one. Between the two poles of laissez faire and overregulation, however, there is middle ground, and the task for policymakers is to identify if there are ways to meet legitimate concerns without damaging the prospects for innovation and growth.

Balkanization as a Symptom of Larger Conflicts

The internet's political transition takes place in the context of a larger shift in international relations. It has become a primary arena for the contest between China, Russia, and Iran on one hand, and democracies on the other. In this contest, democracies are on the defensive. The last decade has not been kind to America, and Europe's decline predates America's woes. There are obvious challengers in authoritarian regimes that prefer a more government-centric internet.

China and Russia are accused of seeking to splinter the internet. This misstates their objectives. They would prefer not to create a new separate internet, but to control the existing one, and cite a desire to protect national sovereignty and public safety as reasons for moving away from the governance regime created by the United States in the 1990s.

In fact, the internet has never been truly open or free for many reasons. Tech giants exercise quasi-government powers. China had planned from the start to design its global internet connections to ensure control and avoid political risk. Russia and Iran follow China's example, and the specter of the Arab Spring and the Color Revolutions drive their efforts to constrain individual rights online. The

argument that these countries should accept political risk in order to maximize economic returns to Western companies is unpersuasive.

It is also worth recalling that internet search engines already filter results, usually without users' knowledge, so what you see now is only **a fraction** of what is publicly available. Users are in effect confined to digital provinces determined by language and location. The difference will be that instead of a search engine company filtering results, filtering could now be driven by political or nationalist concerns.

Additionally, the absence of an effective global mechanism for coordination increases instability. The concern over balkanization comes at a time when global institutions are weakening generally and the tools for collective international action are fracturing. These institutions depended on a powerful transatlantic core that, with Japan, were formed by the West. But power has flowed away from the transatlantic core as Europe's economic and military strength has declined and as U.S. strategic incoherence has increased—a trend that began with the Bush administration and may reflect systemic problems rather than simply bad luck.

The decline of the United States does not mean the rise of China. China's peculiar blend of an ethnic one-party state will not win international support. The United Nations, in its current incarnation, is too weak to impose order. Order requires a degree of comity among the great powers, usually expressed in some kind of binding international commitment, such as those that created the International Monetary Fund, the International Telecommunication Union, or the International Atomic Energy Agency. Disparate governance regimes increase instability, but this is a reflection of the instability produced by competition among powerful states.

Redefining Ideology to Accommodate Digital Sovereignty

Faced with these pressures, change is inevitable. We are in effect redefining the ideology of the internet, including the core concepts that underpin its governance and architecture. There is little consensus on how to do this, but if there is an alternative, it is the emerging contours of the idea of digital sovereignty. Any redefinition must start with a less-romanticized view of cyberspace. While the long-term goal is to ensure privacy, security, and individual rights, the immediate goal is to accommodate the concerns of states to protect their citizens without sacrificing fundamental freedoms.

The key concept for reconceptualization is digital sovereignty. **Digital sovereignty** is the right of a state to govern its networks to serve national interests, the most important of which are security, privacy, and economic health. States impose national law and regulation on networks and services to improve privacy and security, ensure opportunities for their citizens, and, in unpopular regimes, reduce political risk.

The most likely effect of this reconceptualization is an increase in "friction"—inefficiencies produced as a result of constrained connectivity. As sovereign rule increases, connectivity may become more difficult. There are precedents we can look at. Countries have their own currencies, and there are costs to using them in other countries, but it is not impossible. Countries have national telecom service providers, but you can call from one country to another for a fee. The most likely change from the extension of sovereignty will be this increase in friction, making it harder and more expensive to connect across borders.

The problem with this national approach is that the internet and its underlying architecture are global by design. A complex web of commercial connections underpins what we call cyberspace. It is not an aggregate of national networks but a system whose boundaries follow the logic of networks and markets, not politics. It was not designed or built to respect borders. To be effective in this complex web, sovereign

control must be extended beyond a state's jurisdiction and be extraterritorial, but there are not international mechanisms to impose extraterritorial control or to negotiate agreement on common rules.

The growth of sovereignty, accompanied by localization (e.g., government measures that compel companies to store digital data locally within their jurisdiction or provide procurement preferences for national companies and indigenous technology), restricts the ability of foreign companies to compete. Strict data localization laws that require that personal data on citizens or accounting records be stored or processed within a country became more common after 2010. However, the majority of laws that impose restrictions on international data transfers allow data transfers if certain conditions are met. Examples include explicitly requiring the consent of the data subject or restricting export to countries that have laws ensuring "adequate data protection." Data localization laws can be a barrier to companies expanding their international presence, and some companies often lack the personnel or financial and legal resources to develop compliance strategies. However, many governments see trading some potential growth for greater protection of sovereignty as a reasonable exchange.

Sovereignty and localization do not mean, however, that the internet will be "broken." Balkanization is unlikely. The damage to connectivity and commercial interests that would result will deter most countries from this route. A nation could impose new technical standards or protocols for network connectivity that would "fracture" its connection to the global internet, but only at serious economic cost. Some internet users will lose the advantage that untrammeled internet access can provide. The precedent here is China. China's users are denied access to valuable information (Chinese researchers complain of this) and have a view of reality distorted by the Chinese Communist Party, which is meant to serve its interests. But this does not prevent Chinese companies from doing business.

What greater sovereign control means, especially if it is badly designed, is that countries will not extract the full economic benefits from digital connectivity. This is an increasing risk to growth, but other priorities, such as security and privacy, will trump income in setting national priorities. Countries will make a political decision to accept some economic cost to gain the benefit of security and privacy, but none will decide on actions that lead to major fracturing.

Almost 80 countries (including the European Union) have passed laws that restrict the flow of data across borders. Controls on personal data represent the most common form of restriction, followed by financial and accounting data, government data (including some public records or defense-related data), and tax data. Enforcement of these laws varies by country. Data localization will not "break" the internet or result in balkanization. It will complicate companies' business models and likely slow overall growth, falling first on companies with a global presence. The **long-term opportunity cost** is that newer or smaller firms may lose opportunities to service a global market.

Mechanisms to Reshape Cyberspace

The trends reshaping the digital world—decoupling, regulation, militarization, mistrust, and weaponization—are symptoms of larger international problems, including the resurgence of nationalism around the world and the declining power of the global institutions created by the United States and its Western allies. What we are seeing is the extension of sovereign control. But just as nations can have different political systems or even different cuisines, they can still do business with each other. The internet will continue to serve as a platform for global commerce. Airspace is split along national lines, but international air travel is possible, in part because there are international agreements on standards and safety (under the auspices of a UN organization).

The lack of an effective mechanism to coordinate and guide national actions is the central problem for reducing friction and managing the spread of sovereign controls. The United Nations, the logical place to locate such a mechanism, is itself in crisis, and competing powers have suspended meaningful security dialogues. The **UN Secretary-General's High Level Panel** was an effort to remedy this, but it has not gained traction or coherence. Arms control and disarmament are eroding as international tensions increase. The "militarization of cyberspace is a symptom of this, and treating the symptom rather than the root cause is unlikely to lead to improvement. Creating peace institutes or having concerned netizens call for peace does not address the fundamental problem that authoritarian states seek to reshape global rules and institutions to better serve their interests, reduce the power of the West, and inhibit the space of citizens' political action at a time when the Western defenders are enfeebled.

The situation is difficult, not hopeless. Building a mechanism for coordination in cyberspace to avoid balkanization is a first step. This could likely first be a mechanism composed of like-minded states. Privately funded initiatives lack legitimacy. The Paris Call, although a valiant effort, lacked political substance and had procedural problems (one of the major powers declined to sign after being given a "final" text a week in advance for review). The text itself was not compelling. Any effort that fails to win support from India, the United States, Russia, and China cannot be called a success. While a renewed Paris effort this year is more likely to win support from the major democracies, it will not reverse these larger trends.

If there is a precedent, it is unfortunate but may offer instructive lessons. In 1915, concerned about World War I, Henry Ford purchased a ship (christened the *Peace Ship*), assembled a group of clergy and academics (progenitors of today's multi-stakeholder community), and set sail for Europe to press the case for peace. The warring powers received Ford and his compatriots coldly, if at all, and the press ridiculed his effort. Well-meaning **private efforts** carry insufficient weight when the interests of great powers clash, and the earlier age of apparent global digital peace cannot be restored in an environment of increasing conflict.

It is not, however, 1915. These precedents are imperfect. There is already a deep conflict in cyberspace, but it has not yet caused death[1] or destruction. To avert the reception afforded to the *Peace Ship*, three things are needed: a cold recognition of the true nature of cyber conflict and the powerful political disagreements that drive it; the limited space for agreement; and the absence of effective mechanisms for achieving it. This is what drives balkanization as much as the desire for digital sovereignty, and we should not conflate the two

It is possible to manage risk on the internet without closing off commercial opportunity or expanding restrictions on human rights such as free expression. China was an early master of being open for business and closed for politics. Being open for business but closed for politics turns out to be difficult, but not impossible, and in fact the development and availability of technologies that allow governments to exercise greater authority in content and surveillance are increasingly easy to come by. Intelligent technology offers the possibility to allow access to commercial information while managing and restricting access to politically or culturally sensitive information. This kind of cyber sovereignty is not a desirable outcome for those who see the internet as a tool for expanding fundamental freedoms, and ill-conceived approaches to digital sovereignty will harm innovation and economic growth, but both national and multilateral solutions provide an opportunity to mitigate risk and minimize harm.

1. The death of an unfortunate German as they were being transferred from one hospital to another cannot be considered intentional.

It is not that balkanization is increasing, it is that freedom online and off is shrinking. Some balkanization is unavoidable, if by this we mean the establishment of regulatory boundaries, but a core group of democracies can guide this balkanization to address the challenges to privacy, security, and commerce while preserving, at least in their own jurisdictions, fundamental rights. The first step is to articulate a new ideology based on principles that respect both sovereignty and individual rights. This is best embedded in a discourse based on democratic and market-based principles. The second step is to develop a robust mechanism for cooperation among like-minded democracies and use this as a platform to negotiate and avoid risks of damage from balkanization while meeting the legitimate concerns that are reshaping the internet.

The defense of fundamental liberties takes place in the context of political changes the internet has helped create. Citizens now expect to have free access to information and see access to information as a fundamental right. Democratic political discourse is under pressure from increased extremism and polarization that the internet enables. The internet may reinforce nationalism and populism (although we do not wish to overestimate this effect). But it is essential to remember that the same pressures apply to non-democratic states that are ultimately less able to deal with these ailments. The internet increases the fragility of authoritarian states, and their efforts to minimize this should not be allowed to shape a new global internet architecture.

The internet's initial ideology had an ideal of personal freedom at its core, making it the ultimate child of the Enlightenment, and an emphasis on individual rights. The choice before us is not to prevent balkanization but to manage it to defend the internet as a space for individual action—in speech, in data, and in innovation. Any new mechanism must exclude those who are not demonstrably committed to fundamental rights. Seeking consensus with authoritarians is a waste of time. This can be done in the physical space, so it can be done on the internet. ■

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

This report is part of a larger series on the future of the internet.

*A longer version of this paper was drafted for the Observer Research Foundation's "***Digital Debates***."*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.