American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uafp20

Geopolitics and Cyber Power: Why Geography Still Matters

John B. Sheldon

Published online: 03 Nov 2014.

To cite this article: John B. Sheldon (2014) Geopolitics and Cyber Power: Why Geography Still Matters, American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy, 36:5, 286-293

To link to this article: http://dx.doi.org/10.1080/10803920.2014.969174

American Foreign Policy Interests, 36:286–293, 2014
Copyright © 2014 NCAFP
ISSN: 1080-3920 print/1533-2128 online
DOI: 10.1080/10803920.2014.969174

Geopolitics and Cyber Power: Why Geography Still Matters

John B. Sheldon

ABSTRACT Implicit in many analyses of the use of cyber power in international politics and foreign policy is that realist geopolitics no longer matter. Even when the term *geopolitics* is used in such analysis, it is as though the geography has become unmoored from the politics. While there is undoubtedly a geographic foundation to cyberspace because of its physical infrastructure of networked computers, cables, and satellites, it is widely assumed that the geographic setting has no relevance to the political *use* of cyber power by states and non-state actors. This article argues that while cyberspace shrinks time and space in many obvious ways, the geographic setting still matters in the use of cyber power. Further, comprehending the geopolitics of cyber power can help policymakers and analysts understand the identity, motivations, and intentions of actors.

KEYWORDS cyber power; cyberwarfare; geography; geopolitics; information operations; international politics; littoral; urbanization

What role, if any, does cyber power play in classical geopolitics? This question is the inspiration for this article, which seeks to discern the interplay between the use of cyber power—the ability in peace, crisis, and war to exert prompt strategic effect to, from, and in cyberspace—and geopolitics—"the relation of international political power to the geographical setting."[1]

As a phenomenon that is thought to render time and space irrelevant, cyberspace at one point seemed to many to have finally killed off the tyranny of geography and the concept of territorial sovereignty. This irrational exuberance has given way to a quiet, if rather vague, acknowledgment that cyberspace is, indeed, tied to a geographic setting and has geopolitical meaning. Yet analyses about how and why this is the case are few and far between.[2]

The reality is that geography and geopolitics *do matter* and matter a great deal in the use of cyber power. Furthermore, that reality goes well beyond the commonplace fact that the physical segment of cyberspace—the computers, cables, and satellites, among other physical infrastructure—is geographically situated and operated and maintained by human beings who must, by necessity, live on the land in politically organized communities in physically distinct and demarcated territories. Rather, geography and

John B. Sheldon, Ph.D., is the executive director of the George C. Marshall Institute in Arlington, Virginia; founder and owner of the Torridon Group LLC, a space and cyberspace consultancy; senior fellow at the Atlantic Council; and a senior fellow in Global Security Studies at the Munk School on Global Affairs at the University of Toronto in Canada. Prior to his current positions, John was Professor of Space and Cyberspace Strategic Studies at the U.S. Air Force's School of Advanced Air and Space Studies (SAASS) at Maxwell AFB, Alabama. For over six years, John taught the National Security Space course and founded, directed, and taught the Intelligence, Information, and Cyberspace course. A former British diplomat, John holds bachelor's and master's degrees from the University of Hull, UK, and a Ph.D. in politics and international relations from the University of Reading, UK.

geopolitics suffuses cyberspace in most, if not all, of its characteristics and uses around the world and, in fact, exerts influence on how and where cyber power is applied. That this is the case should not come as a surprise since the rise of the information age and all that it has given us has not obviated the fact that, as maritime strategic theorist Sir Julian Corbett noted in the early twentieth century,

> Since men live upon the land and not upon the sea, great issues between nations at war have always been decided—except in the rarest cases—either by what your army can do against your enemy's territory and national life or else by the fear of what the fleet makes it possible for your army to do.[3]

It is only natural and inevitable, therefore, that cyber power should have a significant geopolitical dimension, just like the other strategic domains of land, sea, air, and space power.

Why this reality is underappreciated by many in the cybersecurity and strategic theory field is a matter of general speculation, but what cannot be discounted is the assertion that one reason among many is that the influence of cyber power is less tangible than other forms of power (such as, for example, air power), while, at the same time, is so blindingly obvious that it does not merit even a mention. It is less tangible because in many ways information, the currency of cyber power, cannot be seen directly; blindingly obvious because the hardware that generates, transmits, and receives that information currency is physically ubiquitous and the direct beneficiaries (or victims, as the case may be) are similarly ubiquitous. Just like the nose on our face, we hardly notice the powerful impact information technologies have on our modern existence.

More specifically, however, there is a sense that many in the cyber field have gotten ahead of themselves and, in the process, have become untethered quite literally from the ground. Breathless exhortations of revolutions in military affairs and the unalloyed goodness of the information age have led too many to believe that rather than expected and phenomenally unremarkable changes in the character of war and strategy as a result of the rise of cyber power, we are instead in the midst of some change in the *nature* of things that renders crusty old geography and corrupt geopolitics utterly irrelevant to our endlessly bright future. If only it were so and, even then, taken on its own terms, there is ample philosophical reason to regard that future as less than desirable.

As a partial remedy to this unwarranted optimism and the generally vague notion that geography and geopolitics somehow matter, outlined below are the various ways in which cyber power is suffused by geography and geopolitics and also how the practice of cyber power can impact the geopolitical context. The article examines the geographic and geopolitical implications of the physical infrastructure of cyberspace; the fact that targets in cyberspace have a geographic setting and geopolitical meaning; the rise of megacities along an increasingly urbanized littoral; and the implications for classical geopolitics in the traditions of the great theorists of geopolitics, Sir Halford Mackinder and Nicholas Spykman.

THE PHYSICAL SEGMENT OF CYBERSPACE: FROM CABLES TO THE INTERNET OF THINGS

The physical infrastructure of cyberspace maps the contours of contemporary geopolitics more than we might think and has become even more reflective of geographic and geopolitical realities in the physical realm with the advent of the Internet of Things. All too often the physical infrastructure of cyberspace tends to be treated in (and as) a utilitarian manner devoid of geopolitical context.

The physical infrastructure of cyberspace comprises the land and undersea cables that provide connectivity across landmasses and oceans; communication satellites in low-Earth and geostationary orbits; server farms, routers, and other key hardware dotted all over the world; and the physical locations of key corporate, government and research centers, headquarters, and so forth, such as the physical facilities of computer emergency response teams (CERTs); and computers and other devices used by people worldwide. This infrastructure is vast, complex, interconnected, and covers the globe.[4] Furthermore, the majority of this infrastructure is privately owned, with the rest owned by governments. This is geopolitically significant because it suggests that cyberspace—at least in how it manifests itself in its physical infrastructure—is a global *domain* rather than a global *commons* as is popularly claimed.[5] This reality is increasingly evident with states imposing their sovereignty in cyberspace through enforced legislation and implemented policies that influence to some degree or another how it is exploited by users at the national level.[6] States are also [re]claiming their sovereignty in cyberspace through the promotion of international regimes.[7]

Cables traverse ocean floors and satellites circle the Earth in orbits as high as 22,360 miles above the planet's surface. On land, cabling that literally wires cyberspace usually utilizes existing infrastructure such as railways. Satellite ground stations and antennas are located on land and so, naturally, are subject to the laws of the states that govern those lands. Server farms, including network switches and routers, and data centers are also located on land, often near conurbations and near the large power sources needed to run the thousands of computer servers located therein.

Geographic and political considerations are central to deciding where to place landing points for undersea cabling, such as taking into account transoceanic distances to control costs as well as shipping traffic near the landing point in order to mitigate the risk of a ship tearing the cable.[8] Similar considerations framed decisions about the landing of submarine cables in the late nineteenth and early twentieth centuries. Communication satellites in Earth orbit must maintain their orbital positions and station in what is, in fact, a complex Earth–Moon space terrain comprising the Earth's gravity well, the drag produced by traces of the Earth's atmosphere even at 22,360 miles altitude, as well as the crowded and increasingly contested geostationary "territory" where orbital slots are becoming scarce. Further, the launch of communication satellites can only be done from a handful of locations around the world, with the location of satellite ground control stations chosen based on their ability to send signals to and receive signals from satellites and distribute those signals via terrestrial networks.[9]

Geographic imperatives suffuse the physical infrastructure of cyberspace, and geopolitical considerations further influence the makeup of how cyberspace is created. For example, in the late nineteenth and early twentieth centuries, undersea cabling was dominated by Great Britain and its geopolitical agenda centering around the maintenance of its empire and its domination of global trade. When Britain laid undersea cables across the North Atlantic from the British Isles to North America, it was not just because London felt it necessary to maintain high-speed communications with its Canadian dominion, but was also reflective of the massive British investments in the United States.[10] The proceedings of the Paris Peace Conference in 1919 regarding the disposition of Germany's former cables laid bare just how important this issue was, including for the United States, which was emerging as a global power.[11] Similarly, today the United States and, to a lesser extent, Great Britain can leverage geopolitical advantage through their ability to control the contemporary undersea cable network.[12]

The physical infrastructure of cyberspace is more than just network and civil engineering. It is shaped and influenced by practical geographic imperatives and by powerful geopolitical forces. Its structure is also shaped by the existence and emergence of urban clusters, growing economic power, and military (geostrategic) requirements. These factors gave rise to the cyberspace we have today and will also influence the cyberspace we will have in years to come—not only in terms of network speeds, reliability, and access, but also in terms of the international governance of cyberspace and who, if anyone, controls the Internet.[13]

THE TARGET IS ALWAYS IN THE PHYSICAL REALM

In the continuous back and forth of what many call "cyberwarfare," the shadow of geopolitics and geography also looms large. For starters, and especially with regard to state-to-state (and their proxies) cyber exchanges, geopolitical considerations often determine the targets. Further, the target itself is geographically located in that the computer network penetrated, the data pilfered or otherwise manipulated, and the political, economic, and military significance of that data are owned by and within the sovereign territory of some political entity. As a result, the actual and potential geopolitical implications of cyber exchanges should be obvious, although their overall impact is often mitigated by the challenges posed in attributing the source of a cyber exchange. Attribution, of course, is important and the forensic science behind it is improving rapidly. The problem: the forensics of attribution can rarely, if ever, give immediate results and can take days if not weeks to provide solid technical evidence. Further, what is not always immediately apparent to a victim is that they are under cyber attack, further complicating attribution.

When Iranian officials discovered the Stuxnet virus in the Natanz nuclear processing plant, they had scant technical and physical evidence with which to precisely identify the perpetrator. What was beyond doubt, however, to Iranians and third-party observers alike, was that countries such as Mongolia, Uganda, and Greece, to pick three at random, were not responsible. Instead, given Iranian geopolitics since 1979 as well as publicly strained relations with the United States and Iran's regional neighbors, the prime candidates were identified as being the United States, Israel, certain European countries, and perhaps even the Russians or Gulf Arab states.[14] European countries such as the United Kingdom, Germany, and France would certainly have had the technical and financial wherewithal to mount a Stuxnet-like operation (and history may yet show that any of these may have provided assistance in some way), but not necessarily the political will. The Gulf Arab states, such as Saudi Arabia and the United Arab Emirates, do not have the technical capacity to undertake such an operation, but do have the financial ability to bankroll it. The problem with that theory, however, is that their proximity to Iran would probably have precluded their involvement because of the real possibility of blowback. Last, Russian involvement was very unlikely despite their technical capacity to undertake an operation like Stuxnet because of their substantial commercial and strategic ties to Tehran.

Neither the U.S. nor Israeli governments have officially acknowledged their involvement in the Stuxnet operation, but this has not stopped the Iranian government from assigning blame to both. This charge has since been strengthened by leaks that point to a massive U.S.-Israeli operation that, if the stories are accurate, is remarkable in its scope, expense, and complexity.[15] Further, Iranian officials would have doubtless looked to the United States and Israel as perpetrators given their technical, operational, and financial capacities to undertake such an endeavor, as well as their previously demonstrated political will in confronting Iranian nuclear activities. The larger point here is that interstate cyber exchanges almost always have a discernable geopolitical context that can explain the wider causes behind them.[16]

This point is further emphasized by Chinese espionage through cyberspace. The most prominent targets appear to be high-technology corporations and government programs primarily in the United States, but also in Japan, Canada, Western Europe, and Israel—countries where most of the world's high technology is researched, designed, developed, and manufactured. Hence the obvious geopolitical dimension to Chinese cyber activities in this regard.[17] In the Middle East, cyber exchanges reflect the complex geopolitical dynamics with ongoing hostilities between Israel and Palestinians (and their respective sympathizers), Israel and Iran, and Saudi Arabia and Iran being the most prominent of the tensions and conflicts.[18] Wherever geopolitical rivalries and tensions are present and wherever the physical locus of power resides, cyber exchanges occur. Terrorist use of cyberspace also has a geopolitical dimension in that efforts to raise money and recruit are geopolitically focused toward diasporas and co-religionists who have a geographic footprint.[19] Last, it might even be claimed that the criminal use of cyberspace can have a geopolitical aspect. Just as criminals rob banks because that is where the money is, modern criminals, often taking advantage of countries with cyberspace infrastructure but weak governance, use cyberspace to further their geographic reach and take advantage of global financial networks by focusing their efforts on corporations and publics in wealthy parts of the world such as North America, Europe, Gulf Arab states, and Australasia.

The ubiquity of cyberspace and, in turn, cyber power should not confuse us about the role of geopolitics and geography in its use. In any cyber endeavor the geographic element looms large in that activity must be started by a human being located somewhere geographically, on a machine and network similarly situated. That human being initiates a cyber action for the purposes of national interest, economic imperative, political ideology, perceived religious mandate, and/or criminal intent. The code that will in some manner manipulate data traverses cyberspace through a number of physical entities—natural and manmade—to its target that is also located somewhere geographically. That target comprises machines and networks used by humans (or even a targeted individual) who also reside somewhere that can be found on a map. Invariably, there is a geopolitically symbiotic relationship between both geographically situated ends of the cyber exchange. That symbiotic relationship has geopolitical meaning that can be discerned through the study of traditional, or classical, geopolitical thought that dates back to Thucydides, via the works of Halford Mackinder and Nicholas Spykman, through to the likes of Jakub J. Grygiel and C. Dale Walton today.[20]

URBAN GEOGRAPHY AND CYBER POWER: THE RISE OF THE MEGACITY

The ubiquity of cyberspace, and, therefore, the potential for the practice of cyber power, is hardly uniform in its geographic coverage. There are still, and will remain, places on Earth where cyberspace will be difficult to access or in which its penetration in a population will be shallow at best. Changes currently under way in economics, demographics, as well as political decisions affecting issues such as agriculture, city planning, and the building of infrastructure, are all creating a growing trend of massive urbanization throughout the world and the creation of megacities.[21] This mass urbanization has significant implications for cyberspace in terms of its physical infrastructure as well as its use.

Mass urbanization will likely result in global clusters of cyber activity that will also have their own geopolitical narratives and imperatives. Further, while the global cyber infrastructure that will link these clusters will probably be technically uniform, and perhaps even subject to some form of global governance, the infrastructure within these clusters of megacities will most certainly not be. Rather, the cyber infrastructures in these megacities—especially in the developing world—will likely be a hybrid mix comprising hardware from commercial carriers on one hand and improvised, often illegally acquired, hardware and networks jury-rigged by technically competent individuals in particular neighborhoods and communities within a megacity. This phenomenon is already under way in cities such as Mumbai, Karachi, Accra, and Nairobi, and will only expand in the coming decades given the ever-lower bar for entry into cyberspace,[22] as well as the challenges that persist with regard to curbing illicit practices in electronic waste disposal.

The rise of the megacity is taking place concurrent with the advent of the Internet of Things, as well as the emergence over the past decade or so of so-called smart cities. Both of these technical trends have tremendous geopolitical and geographic implications for cyber power as the twenty-first century unfolds.[23] Geopolitically, new centers of power will emerge along with megacities, the vast majority of which will be within 100 miles of a coastline and in many will contain large elements of potential instability because of poor or partial governance and large economic inequalities. Further, with the growing number of people moving from rural areas to more crowded conurbations, issues of food security will become more acute as local agricultural sectors shrink in size and foodstuffs must be imported from abroad. This leads to potentially fragile supply lines into megacities because of potential disruptions ranging from the everyday economic challenges of supply and demand through to deliberate interference such as embargoes, piracy, or the cyber interdiction of logistical networks.

Geographically, the emergence of megacities is largely occurring along the littorals of Eurasia, Africa, and Latin America, with the result that more than 70 percent of the world's population will live within 100 miles of a coastline by 2050.[24] As well as megacities becoming cyber hubs of regional networks, we are also likely to see the merging of cyberspace and the maritime domain. In many ways, this trend is already under way with the digitization of maritime transportation and policing and with the more advanced of the world's navies already adopting and integrating cyberwarfare into their policies, doctrines, and tactics, and techniques and procedures (TTPs). This adoption and integration of cyber effects and fires will further expand, and change, the influence of maritime power against the urbanized littoral. Conversely, more advanced parts of the urbanized littoral, leveraging their own cyber power that is integrated with sea and air defenses as well as maritime-domain-awareness networks, will be able to counter attempts to impose offensive maritime power. Such circumstances point to the urbanized littoral as the focal point of stand-alone cyber conflict, with implications for maritime trade and law and order, as well as cyber-enabled military conflict that can enhance the attributes of maritime force on the one hand and land-based forces on the other. The ability to seize and sustain some semblance of information superiority will likely provide the advantage in struggles over the urbanized littoral and its maritime approaches.[25]

This increasing urbanization of the littoral, along with the growing ubiquity of cyberspace within it, will change the character of war in other ways as well. If strategic thinkers like David Kilcullen are right, urban warfare will become the norm in the emerging strategic environment and will prominently feature cyber power and its attendant integration as a decisive domain.[26] As a result, the armed forces—armies, navies, and air forces—of many of the world's developed regional and great powers are training for urban warfare where friendly and adversarial cyber power will be a major element of the operational environment in peace, crisis, and war.[27] This emerging phenomenon will likely see innovations in TTPs, defensive and offensive technologies, and operational concepts appropriate to the complex urban environment where cyber power is ubiquitous. These innovations and operational concepts will probably involve the ability to disrupt, deny, and otherwise manipulate local networks; conduct psychological and other information operations in digitally rich and complex geographies; and conduct sophisticated deception-and-denial operations against adversaries and neutral audiences. Indeed, the 2014 conflict between Israeli Defense Forces and Hamas in Gaza will probably be seen as one of the progenitors of this kind of warfare where the brutalities and horror of war in a crowded, complex urban environment are combined with an endlessly contested and chaotic information environment.

BLURRED LINES: THE HEARTLAND, PIVOTS, AND RIMLANDS AND CYBER POWER'S INFLUENCE ON GEOPOLITICS

On a global scale, cyber power is very unlikely to change the nature of the eternal geopolitical struggle between continental and maritime powers. This struggle centers around the idea that developments in transportation technologies (e.g., railways, ship propulsion, air power) and thus the means with which to project military force over long distances can determine the relative superiority of the Heartland continentalist powers over the Pivot, or Rimland, maritime-oriented powers. Propounded by early geopolitical theorists Sir Halford Mackinder and Nicholas Spykman, the Heartland is located on the Eurasian landmass and has moved eastward over the past 100 years from Germany, then to the Soviet Union/Russia, and, in the coming decades, is likely to shift to China. The Heartland has access to an abundance of resources and, with modern transportation, such as railways, can leverage those resources into potentially overwhelming economic and military power. This can (and in the past has) led to a challenge to the global balance of power, and so offshore powers such as the United States and Great Britain must use their maritime power to prop up the littoral of the Eurasian landmass—the Rimland—to prevent the Heartland from gaining dominance.[28] Since the end of the cold war, this geopolitical approach has generally receded from the considerations of policymakers, but with recent geopolitical perturbations in Eurasia it is likely to enjoy a newly found applicability.[29] Cyber power can enhance, even critically enhance, the criteria for geopolitical success on a global scale, but is unlikely to change the nature of this grand competition.

The geopolitical frameworks of Sir Halford Mackinder and Nicholas Spykman still have relevance in today's world and can easily accommodate the rise of cyber power that has occurred over the past few decades.[30] Looked at from the grandest of scales, the competition between the United States and its Western allies on one hand, and Russia, China, and their respective allies on the other, is, in essence, a continuation of the competition over whether the geopolitical Heartland can achieve superiority over a geographically dispersed Rimland along the littoral. Cyberspace is suffused throughout both the Heartland and Rimland regions, but because of the growing urbanization along the littoral, the strategic expression of cyberspace—cyber power—will be more pronounced.[31]

Diplomacy, economic statecraft, and land, sea, air, and space power still matter in the twenty-first-century geopolitical competition, but we can add to this list of areas of competition the realm of cyberspace. What makes cyber power unique in geopolitics is its influence not only as an instrument of power in its own right, but its direct (as well as indirect) influence on the other, more traditional, instruments of power. Throughout history, all instruments of power have influenced other instruments to some degree or another, thus changing the character of these instruments and how their power is exploited. For example, diplomacy has long had an influence on trade, and vice versa; in warfare, the influence of air power in the first half of the twentieth century had tremendous implications for sea power; and the rise of space power in the latter half of the twentieth century has had a significant impact on the conduct of warfare in the other domains. The influence of cyber power, in its own right as well as on other instruments of power, is so profound that it has changed not only the character of warfare in all the other domains, but has also changed the character of diplomacy, economics, and the expression of culture, while, at the same time, providing yet another, albeit pervasive, tool with which states compete with one another in various locations and over any number of issues.[32]

This urbanized littoral is where the continuing grand geopolitical struggle between the Heartland and Rimland powers will take place and will be expressed in both traditional and nontraditional ways. And, in these very same geographic and geopolitical contexts, cyber power may prove to be an instrument of power that could give the decisive edge in that struggle—with the advantage going to the side better able to exploit cyberspace for information operations, provide superior information assurance, and coherently integrate cyber power into all other instruments of power.

CONCLUSION

This article has demonstrated that both geography and geopolitics exert tremendous influence on cyberspace and that, in turn, cyber power—the strategic effect generated from cyberspace—has geographical and geopolitical meaning. Far from being everywhere and nowhere, cyber power, while unique in its technical character, is nothing new under the geopolitical sun.

Notes

1. Saul B. Cohen, *Geography and Politics in a Divided World* (London: Methuen, 1964), 24.
2. For an exception to this, see the following exchange of views: Colin S. Gray, ''The Continued Primacy of Geopolitics,'' *Orbis* 40, no. 2 (1996): 247–259; and Martin C. Libicki, ''The Emerging Primacy of Information,'' *Orbis* 40, no. 2 (1996): 261–274.
3. Julian S. Corbett, *Some Principles of Maritime Strategy* (London: Longman, Greens & Co., 1918), 12.
4. By far the best treatment to date of the physical infrastructure of cyberspace is Andrew Blum's *Tubes: A Journey to the Center of the Internet* (New York: Ecco, 2012).
5. See John B. Sheldon, ''The Rise of Cyberpower,'' in *Strategy in the Contemporary World*, 4th ed., ed. John Baylis, James J. Wirtz, and Colin S. Gray (Oxford: Oxford University Press, 2013), 310–311.
6. See Chris C. Demchak and Peter Dombrowski, ''Rise of a Cybered Westphalian Age,'' *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32–61.
7. For example, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security emphasizes that states can assert sovereignty in cyberspace. See *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* A/68/98 (New York: United Nations, June 23, 2013), http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.
8. See Andrew Blum, ''Netscapes (WIRED),'' http://andrewblum.net/2009/netscapes-wired-magazine/.
9. See Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (London: Frank Cass, 2002), 60–85.
10. See, for example, Niall Ferguson, *The Cash Nexus: Money and Power in the Modern World, 1700–2000* (New York: Basic Books, 2001), 296–299.
11. See U.S. Department of State, Foreign Relations of the United States, *Papers Relating to the Foreign Relations of the United States, The Paris Peace Conference, 1919*, vol. 4, ''Minutes of a Meeting of the Council of Four'' (Washington, DC: U.S. Government Printing Office, 1919), 494–500. See also P. J. Hugill, ''The American Challenge to British Hegemony, 1861–1947,'' *The Geographical Review* 99, no. 3 (July 2009): 403–425.
12. On the geopolitics of British undersea cabling, see, among others, P. M. Kennedy, ''Imperial Cable Communications and Strategy, 1870–1914,'' *The English Historical Review* 86, no. 341 (October 1971): 728–752.
13. On the ongoing struggle to preserve Internet neutrality and to keep control of the global cyberspace domain out of the hands of sovereign states, see Laura DeNardis, *The Global War for Internet Governance* (New Haven, CT: Yale University Press, 2014).
14. On the initial uncertainty of Iranian officials about who was behind the Stuxnet attack, see William Young and Robert F. Worth, ''Bombings Hit Atomic Experts in Iran Streets,'' *New York Times*, November 29, 2010, http://www.nytimes.com/2010/11/30/world/middleeast/30tehran.html?_r=2&hp&.
15. See Greg Miller and Sari Horwitz, ''Justice Dept. Targets General in Leak Probe,'' *Washington Post*, June 27, 2013, http://www.washingtonpost.com/world/national-security/justice-dept-targets-general-in-leak-probe/2013/06/27/9ad8bc4e-df7c-11e2-b2d4-ea6d8f477a01_story.html.
16. To date, the most authoritative account of the Stuxnet attack can be found in David E. Sanger's *Confront and Conceal:*

Obama's Secret Wars and Surprising Use of American Power (New York: Crown, 2012), 188–225.

[17] On the use of cyberspace for espionage, see Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011).

[18] See Terry Pattar, ''Cyber Attacks in the Middle East,'' *Current Intelligence* 5, no. 3 (Summer 2013), http://www.currentintelligence.net/analysis/2013/7/29/cyber-attacks-in-the-middle-east.html.

[19] On terrorist uses of cyberspace, see, among others, Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006).

[20] See Robert B. Strassler, *The Landmark Thucydides* (New York: Touchstone Books, 1996); Halford J. Mackinder, *Democratic Ideals and Reality* (London: Faber and Faber, 2009; first published in 1919); Nicholas J. Spykman, *America's Strategy in World Politics: The United States and the Balance of Power* (New Brunswick, NJ: Transaction Publishers, 2007; first published in 1942); Jakub J. Grygiel, *Great Powers and Geopolitical Change* (Baltimore, MD: The Johns Hopkins University Press, 2006); and C. Dale Walton, *Geopolitics and the Great Powers in the Twenty-First Century: Multipolarity and the Revolution in Strategic Perspective* (Abingdon, UK: Routledge, 2007).

[21] On the rise of megacities, see Frauke Krass, Surinder Aggarwal, Martin Coy, and Günter Mertins, eds., *Megacities: Our Global Urban Future* (Dordrecht, Netherlands: Springer, 2014).

[22] On this, see Scott Smith, ''Shanzai! The Era of DIY Warfare,'' *Current Intelligence* 3, no. 8 (August 2011), http://www.currentintelligence.net/columns/2011/7/18/shanzai-the-era-of-diy-warfare.html.

[23] On smart cities, see Anthony M. Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* (New York: W. W. Norton, 2013).

[24] On the increasing urbanization of the world's population up to the year 2015, see Department of Economic and Social Affairs, Population Division, *World Urbanization Prospects: The 2011 Revision* (New York: United Nations, 2011), http://esa.un.org/unup/pdf/WUP2011_Highlights.pdf; on urbanization along the littoral, see National Intelligence Council, *Global Trends 2025: A Transformed World* (Washington, DC: National Intelligence Council, 2008), 23.

[25] For an initial exploration of this issue, see Peter Dombrowski and Chris C. Demchak, ''Cyber War, Cybered Conflict, and the Maritime Domain,'' *Naval War College Review* 67, no. 2 (Spring 2014): 71–97.

[26] See David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerilla* (New York: Oxford University Press, 2013).

[27] See, for example, the Australian Army, *Future Land Warfare Report: 2014* (Canberra: Directorate of Future Land Warfare, April 2014); and Paul McLeary, ''US Army Sees 'Megacities' as the Future Battlefield,'' *Defense News*, August 30, 2014, http://www.defensenews.com/article/20140830/DEFREG02/308300027/US-Army-Sees-Megacities-Future-Battlefield.

[28] See Mackinder, *op. cit*., and Spykman, *op. cit*. Mackinder promulgated the concept of the Heartland, whereas Spykman believed that Mackinder exaggerated its potential power. Spykman promulgated the concept of the Rimland, arguing that it was susceptible to the influence of offshore maritime powers, thus hemming in any dominant Eurasian power. Also implicit in these theories is that Heartland powers tend to be prone to authoritarianism, whereas offshore powers tend to be liberal democracies.

[29] On these geopolitical perturbations, see Walter Russell Mead, ''The Return of Geopolitics: The Revenge of the Revisionist Powers,'' *Foreign Affairs* 93, no. 3 (May/June 2014): 69–79.

[30] See Colin S. Gray, ''In Defence of the Heartland: Sir Halford Mackinder and His Critics a Hundred Years On,'' *Comparative Strategy* 23, no. 1 (Spring 2004): 9–25.

[31] See Walton, *op. cit*.

[32] See, for example, John B. Sheldon, ''Deciphering Cyberpower: Strategic Purpose in Peace and War,'' *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 95–112.