Anh Phuong Nguyen
Professor Stuart
INST 500
March 10, 2016

The Ascendance of Geoinformation

America in a Geoinformational Landscape

The Information Age. That is the legacy of the 21st century: The marriage of computers and telecommunications has ushered in a revolution that is rocking the power structure of the international system. Information now transcends borders and boundaries, flowing from one end of the world to another. Some promoters of the information revolution argue that the huge impact of this global dissemination of information is upon us: Distance will be irrelevant, and geography, as a consequence, dead. But while we may be witnessing the shrinking of distance, geography is a reality that will not go away. Napoleon is once rumored to have said, "Geography is destiny" before deciding to invade Russia; this statement is still true, although the concept of geography has been expanded. In the 1990s, the concept of market geography surfaced, and it, along with the physical geography, helped craft a country's destiny. The struggle for space still continues in our era, but the battlefield now encompasses the sphere of information and its most important sub-region, cyberspace.

Geoinformation thereby emerges to parallel geostrategy and geoeconomics as a new geopolitical approach. It is also a concept that encourages an active incorporation of information into the calculations of grand strategy. As the birthplace of the Internet, the United States benefits from a first-mover advantage and dominates the map of geoinformation. But this monopoly is starting to erode as other actors cry for a new balance of information and attempt at reshaping the architecture of the infosphere. It is the great irony of the Information Age: "…the very technologies that empower

[America] to create and to build also empower those who would disrupt and destroy."[1] A new great game for influence is underway, and the United States needs to reassess its place in the new world to bring this game to an end that is favorable for all.

PART A: The Ascendance of Geoinformation

Infosphere

Geoinformation is the conjunction of two realities—those pertaining to the impacts of geographical space on strategic calculations and those recognizing that information is now an object of conflict and cooperation. "Geography," Spykman once wrote, "does not argue; it just is."[2] In this regard, geography can generally be understood as a physical reality with a tangible resource space. Information, on the other hand, has a diverse range of more abstract interpretations, and no single conception would satisfactorily convey the meaning of the word. By merging these two notions, this neologism advocates for the acknowledgement of an information geography, or infosphere, inhabited by informational entities (both offline and online, analog and digital, carbon-based and silicon-based), as a space "out there" that, instead of diminishing the role of geography, extends the concept of geography: infosphere is a hybrid realm that includes both the material elements (e.g., libraries, bookstores, etc.) and the immaterial elements (e.g., database, media, etc.) This space is ever-shifting, "constructed and continually reconstructed for and by the movement of information."[3]

The notion that infosphere is a new arena for contestation or cooperation rests on the presumption that states and non-state actors pursue power in one way or another and the main

---

[1] THE WHITE HOUSE. Office of the Press Secretary. "Remarks by the President on Securing Our Nation's Cyber Infrastructure." News release, May 29, 2009. The White House. Accessed May 15, 2016. https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[2] Spykman, Nicholas J. "Geography and Foreign Policy, II." *The American Political Science Review* 32, no. 2 (April 1938): 236.

[3] McDowell, Stephen D., Philip E. Steinberg, and Tami K. Tomasello. *Managing the Infosphere: Governance, Technology, and Cultural Practice in Motion*. Philadelphia: Temple University Press, 2008, 11.

resource in infosphere, information, is power. Power, like many popular concepts, has many meanings. In International Relations, power is predominantly defined as "the ability of A to get B to do something he or she would otherwise not do. In the case of authority, B's behavior is driven by obligation, not force, but the operative condition is the same: B does something he or she would otherwise not do because of A's will."[4] But this simple definition turns out to be quite complex: What factors constituting power can shape other actors' behavior? In other words, how can A exercise, or utilize, power in a way that influences how B will respond? Boulding approaches the dynamics of power by presenting three images associated with it: the stick, the carrot and the hug.[5] Power, according to Boulding, can be used to destroy, to produce, and to integrate. This tripartite practice of power shapes the essence of power itself; information is power because it has the ability to cause destruction, to accumulate wealth and to bring about integration.

Power of destruction refers to the use of some punitive measures against structures or persons that the other side values in order to force the target to accede to specific demands. Aerial bombings and nuclear weapons are examples of destructive power, for they have the potential at least to destroy the whole earth. In the information-centric era, information is the ammunition of war. The advent of cyber warfare, or the attacks waged via cyberspace that target an enemy's information systems, can cause destruction to the infrastructure of a country. Like other weapons, the threat from cyber operations is devastating; but unlike other weapons, the cost to launch such attacks is affordable to most nations.[6] In 2007, during a diplomatic dispute with Russia, Estonia suffered from a massive cyber attack on both its public and private networks. Hackers bombarded Estonia's Internet infrastructure

[4] Dahl, Robert. "The Concept of Power." *Behavioral Science* 2, no. 3 (1957), 202.
[5] Boulding, Kenneth E. *Three Faces of Power*. Newbury Park, CA: Sage Publications, 1989, 10.
[6] Schaap, Arie J. "Cyber Warfare Operations: Development and Use Under International Law." *Air Force Law Review* 64 (2009): 134.

with "stream of data packets" that caused major disruptions in service and communications.[7] In a matter of hours, government communications were shut down. The websites of banks, newspapers and broadcasters were crashed. Estonians could not call the emergency services or communicate with the outside world. The damage from this attack was estimated to be approximately 15 billion euro GDP at that time, roughly 5 percent of Estonia's economic activity during the relevant period.[8] No state had claimed responsibility for the attack, but a group of members associated with the Kremlin-backed youth movement accepted responsibility without any state involvement.[9] Of course, on the surface, offensive cyber operations do not qualify to be in UN "armed attacks" categories, or attacks that by kinetic weapons such as missiles or bombs.[10] However, as states rely more and more on their digital infrastructures, non-kinetic consequences of cyber attacks, including disturbing the critical information infrastructures, wiping or stealing sensitive information, can cripple a country as much as kinetic weapons. As Former Secretary of Defense Leon Panetta once warned the international community of the grave threat to national security posed by cyber attacks:

> "[Through cyberspace], attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a 'cyber Pearl Harbor'. An attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."
>
> —Leon E. Panetta., "Defending the Nation from Cyber Attack" (speech, New York, NY, October 11, 2013), U.S. Department of Defense, http://archive.defense.gov/speeches/speech.aspx?speechid=1728

In the past, material resources were dominant in national growth, prestige and power, but with the age of information comes the emergence of information economy, or knowledge economy, where

---

[7] Li, Sheng. "When Does Internet Denial Trigger the Right of Armed Self-Defense?" *Yale Journal of International Law* 38, no. 1 (2013): 180. Accessed May 15, 2016. http://ssrn.com/abstract=2226793.
[8] Ibid., 201
[9] Clover, Charles. "Kremlin-backed Group behind Estonia Cyber Blitz." *Financial Times*, March 11, 2009. Accessed May 15, 2016. http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz48l5oqcKk.
[10] Silver, Daniel B. "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter." Edited by Michael N. Schmitt and Brian T. O'Donnell. *Computer Network Attack and International Law* 76 (2002): 88.

a new source of wealth that generates the most significant returns is knowledge-based information. It is an economy where information is both a currency and a product. Accumulating wealth has been a way to consolidate power, and the information dominance opens a new path to prosperity: the pursuit of wealth is now largely the pursuit of intellectual capital or products of the mind. Unlike other resources, intellectual capital is inexhaustible and grows through application. It defies the law of diminishing returns that governs the traditional factors of production (i.e., land and labor): every additional unit of knowledge (or information) results in a marginal increase, instead of decrease, in performance and value. A state that effectively exploits this new engine of growth can ultimately maintain its long-term competitive advantage and enhance its economy enormously.

The last face of power, the hug, argues Boulding, is the most potent in comparison to the other forms of power, the stick (destructive power) and the carrot (productive power). Integrative power is the ability to federate, the glue that binds society together. It has the greatest potential to persuade people and coordinate social behavior. This kind of power plays a dominant role in the three-legged stool that builds up the bedrock of power. Integrative power, by constructing and facilitating social relations, constitutes legitimacy, and without legitimacy, both threats and riches are feeble, or in Boulding's words, "naked."[11] Integrative power relies on and creates communication—the process of transferring information from one place to another. The process can be verbal or non-verbal, written or visualized. In whatever form, information thrives on humans' insatiable need to know: People always reach out to grab information, and the information gained through communication will, in return, "reach" people's consciousness and contribute to their awareness of the broader and narrower environment around them. This informative experience will influence, to some extent, people's modes of thought and behavior. If the same information is distributed widely enough, it will form a universal

[11] Boulding, Kenneth E. *Three Faces of Power*. Newbury Park, CA: Sage Publications, 1989, 10.

consciousness that forms certain feelings of obligation or responsibility among people—the much-needed legitimacy to carry out both the stick and carrot.

And nowhere in the infosphere is information more integrative than cyberspace, the paraspace imagined by William Gibson in his science fiction novel *Neuromancer.*[12] John Perry Barlow further popularized the term and provided an electronic manifestation of a space behind the computer screen where incorporeal relationships will replace the physical presence and within which "anybody, anywhere can express to the rest of humanity whatever he or she believes without fear."[13] But in the 21st century, cyberspace is not a science fiction; it is a science fact. The reality of a cyber realm promises to transcend the physical barriers that separate societies: Information can now travel globally to build knowledge-based societies and engage everyone in a global conversation. The transportation infrastructure in the world of bits is also significantly different from that in the world of atoms. Internet, the skeleton of cyberspace, has become the main "information superhighway" in this virtual space. Its traffic is information and the vehicles that help navigate the electronic byways are the cables and microwaves that transfer data throughout the net and link all individual hosts under a global system of Internet Protocol (IP) networks. Information moves easily from one place to another, and if it encounters one route clogged with traffic jam, it will find an alternate route to go through and still reach its destination very quickly.

Given the fluidity and ubiquity of this virtual realm, cyberspace is rapidly becoming a new context for interstate interactions and for the conduct of statecraft and diplomacy. But governments soon find themselves struggle to incorporate the cyber dimension into their governance practice. "The Internet is naturally anti-sovereign…and too widespread to be controlled by a single government."[14]

---

[12] Gibson, William. *Neuromancer.* 1st ed. Ace, 1984.
[13] Barlow, John Perry. "Thinking Locally, Acting Globally." *Time*, January 1996. Accessed April 20.
[14] Ibid.

In 1996, Barlow claimed in his *Declaration of the Independence of Cyberspace* that the civilization of the mind in cyberspace will eventually replace the politics of the "flesh and steel," of sovereignty and national boundaries.[15] Since 1648, the state-centric and territory-based Westphalian model has been the salient feature of international order. Cyberspace directly challenges this anchored territorial-state system by resisting the laws that define the Westphalian era: (1) state is the most important actor in international politics, and (2) a sovereignty state is an entity that can exercise supreme authority over its territory. The interconnectivity and integration in cyberspace guarantees that the state will lose its monopoly on power. In fact, the state is only the latecomer to the domain as cyberspace is constructed and has always been managed by the private sector.[16] Moreover, exercising sovereignty over the digital territory proves to be extremely difficult, especially when this geography does not seem to be bound by borders, the main and dominant focus of territoriality.

A corollary question is: Will cyberspace render the conventional international system irrelevant? The answer is no. Traditional principles of sovereignty are still applied to the virtual universe. Although cyber realm is usually characterized by anonymity, it is still subject to the power of states. Cyberspace cannot exist without a physical architecture (i.e., computers, cables, satellites, etc.), and it is important to bear in mind that this physical segment is usually tied to a geographic setting owned, operated and maintained by governments. Borders in cyberspace still exist, albeit less noticeable: IP addresses and Domain Names act as virtual boundaries, although they are not always based on the geography of nation-states. However, in some Asian countries, IP addresses and Domain Names are distributed on a national basis, and switching from a dot-com domain to, for instance, a dot-cn domain has certain jurisdictional implications, as if crossing a virtual border between states.

---

[15] Barlow, John Perry. "A Declaration of the Independence of Cyberspace." *New Internationalist*, no. 479 (January 1996): 27.

[16] Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press, 2012, 15.

The applicability of the principle of Westphalian sovereignty to cyberspace, however, does not necessarily entail that the rules and conduct in the real world will have the same interpretations in virtual realm. States are still the main actors, although the novel nature underlying cyberspace leads to growing complexity of international relations, not only in terms of players, but also in terms of challenges and opportunities. The trajectory of conflict and cooperation in cyberspace is thus envisioned and approached differently. A lot of cyber-related matters now generate opportunities for collaboration among nation-states: the adherence to global norms and practices of cyber governance such as the formulation of cyber treaties (e.g., the Convention on Cybercrime, the International Telecommunications Regulations, etc.) or the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) as the institution responsible for the governance of the Internet.[17] However, cyber venues cannot be devoid of potential contestations that arise when interests of different groups are entangled: the dispute over the Internet architecture (net neutrality, layers principles, etc.), the danger of cyber espionage and the possibility of cyber threats to national security.[18]

The Holy Trinity

Geography has always illuminated politics, and the use of geography in decision-making gives birth to geopolitics, which, as Kurth has put it, is the study of the "realities and mentalities of the localities."[19] The geography in the world today is not simply a product of nature but rather a product of constant power struggle among nation-states, represented by the distribution of spaces in world politics. Despite having a long intellectual tradition, geopolitics has invoked intense criticism and intellectual outbursts since its inception. In 1954, the late geographer Richard Hartshorne condemned geopolitics as an "intellectual poison" and associated geopolitical reasoning with Nazi spatial

[17] Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press, 2012, 159-168.
[18] Ibid., 127.
[19] Granieri, Ronald J. "What Is Geopolitics and Why Does It Matter?" *Orbis* 59, no. 4 (2015): 491-504. Accessed April 20, 2016. doi:10.1016/j.orbis.2015.08.003.

expansionism.[20] At the end of Cold War, there was talk that globalization would lead to supersession of geopolitics by geoeconomics. With the advent of the Information Age, the concept of geopolitics appears obsolete in a world that is increasingly depicted by non-territoriality and immateriality. But these intellectual rejections cannot deny geography's historic entanglement with state power. Geography is never unmoored from politics, but the increasing complexity of international system calls for new interpretations of geography that are reflective of emerging realities. Geostrategy, geoeconomics and geoinformation are three branches of geopolitics that represent the multiplicity of possible political and social constructions of geography. Each geography of governance has its own grammar of actions, and a state that knows how to advance national interests in three arenas will reach the ultimate domination of space and get to chart the globe in its image.

Geostrategy is the most widely acknowledged subfield of geopolitics. Driven by calculations of geography, geostrategists embrace a nationalistic approach to geography, viewing the world from a state's perspective. The geostrategic map is similar to the conventional map composed of spaces contained by borders and separated by oceans. This map indicates a country's geographical location and how a geostrategy can help a country utilize its limited resources to gain command over geographic spaces. Like geostrategists, geoeconomists also look at their own map for guidance, but unlike its geostrategic counterpart, the geoeconomic map is the map of world trade. Major trade blocs such as North American Free Trade Association (NAFTA), European Union (EU), future Asian Trade Bloc (CEPEA or ASEAN+6), etc. become more influential actors in the shaping of the global map. The world is not a static, black-and-white chessboard of an us-versus-them logic. Rather, the globalization system is always in flux—an "inexorable integration of markets, nation-states and technologies to a

[20] Hartshorne, Richard. "Political Geography." In *American Geography: Inventory and Prospect*, edited by P. James and C. Jones, 211-14. Syracuse, NY: Syracuse University Press, 1954.

degree never witnessed before."[21] Nation-states vie for spaces in the market economy, constantly improving their economic capacity in the global marketplace. The quest for markets, rather than resources, becomes the essence of geoeconomic era. Spatial economic structuration depends on the share of global economy; in other words, the big geoeconomic question that a state should ask itself is, to what extent can it rely on domestic economic infrastructure to influence the global geoeconomic architecture and pursue its own strategic goals?

The last geography—tbe sphere of information—is a space formed by informational entities. Generally, the realm of information includes the aggregate of all information systems and information itself: broadcast, print, public libraries, intelligence, etc. When telecommunication and computing step into the information age and create cyberspace, the most recognizable and accessible terrain, the digitalization of information makes information transmission happen within seconds. This transnational aspect of cyberspace undermines a state's control of information flow within its territory, although cyberspace is still subordinated to the statist presence. The power equation thus lies in how much a state can manipulate and regulate the flow of information, how much it can construct appropriate dams or canals to channel this flow to those who need it,[22] and most importantly, how much it can protect its flow from pollution caused by outside factors. The problem is, information in cyberspace, by nature, flows beyond, not within borders and boundaries. Information is too precious to be governed by anarchy, but the fluidity and openness of this flow also bring in dynamics that can create the desired information-rich, knowledge-based societies. In other words, as much as a state wants to sustain the monopoly on information, it cannot resist, and to some extent, does not want to resist, the penetration of the global information flow. This tension ultimately forms the paradox of

[21] Friedman, Thomas L. *The Lexus and The Olive Tree: Understanding Globalization*. 1st ed. New York: Farrar, Straus, Giroux, 1999, 7.
[22] Davenport, Thomas H., Robert G. Eccles, and Laurence Prusak. "Information Politics." *MIT Sloan Management Review*, October 15, 1992. Accessed April 20, 2016. http://sloanreview.mit.edu/article/information-politics/.

sovereign authority in the informational milieu: Information is encouraged to travel abroad while constantly being forced to stay within.[23]

The "pluralization of geography" is an inevitable consequence of the increase in spatial perspectives.[24] Identifying the challenges and opportunities in each geography is thereby essential to the strategic formulation of national interests. Geopolitics, precisely because it is preoccupied with the relation of politics to geography, is at the heart of these calculations, although the traditional geopolitical emphasis on a physical map has been extended to include the ascendance of market and information geography. The "geographical pivot of history" is here to stay, but the seats of power will not just be "natural" as Mackinder claimed them to be.[25] The geoeconomic and geoinformational maps can empower actors who have been marginalized by their physical locations. Constant movements in market and information arenas are likely to precipitate the power transfer among states and non-state actors, and interstate equilibrium is challenged and altered more frequently. That the global landscape is not confined by borders and boundaries is now a fact, but it will, by no means, turn geopolitics into a relic of the past. The "flat world" caused by globalization may lead to the shrinking, eventually the death, of distances, but it will never be the end of geography.

[23] Lundborg, Tom. "What Lies Beyond Lies Within: Global Information Flows and the Politics of the State/Inter-State System." *Alternatives: Global, Local, Political* 36, no. 2 (May 2011): 113.
[24] Tuathail, Gearoid O., and Simon Dalby. *Rethinking Geopolitics: Towards a Critical Geopolitics*. New York: Routledge, 2002, 2.
[25] Mackinder, H. J. "The Geographical Pivot of History." *The Geographical Journal* 23, no. 4 (April 1904): 421-37. doi:10.2307/1775498.

PART B: America in a Geoinformational Landscape

Information Imperialism

> "Last month, when I was in Central Asia, the President of Kyrgyzstan told me his eight-year-old son came to him and said, 'Father, I have to learn English.' 'But why?' President Akayev asked, 'Because, father, the computer speaks English."
>
> —Al Gore, "Remarks by Vice President Al Gore" (speech, Los Angeles, California, January 11, 1994), https://www.uibk.ac.at/voeb/texte/vor9401.html

On June 20, 1897, Queen Victoria celebrated the 60th anniversary of her accession. Millions of people flocked to London to witness her Diamond Jubilee parade: Spectators had arrived early, rented spaces on the rooftop or even slept on the sidewalk days before the celebration. The Royal Navy had their best on show: 165 ships drew up in long lines at Spithead; their names showcased the influence of an empire: Victorious, Majestic, Renown, Powerful, Terrible and Mars.[26] Their presence was undoubtedly awe-inspiring: No better illustration of a maritime power would have been conceived. When Britain had the sea at her command, she reached the zenith of imperial might. To people gathering in London that day, it must have seemed as if the sun would never set on England.

A century has passed, and another empire has arrived. In the 21st century, what this imperialist nation controls is far more powerful than the sea: The "ocean of information," or cyberspace, now rises to prominence as a new arena for global conduct. The embrace of cyberspace is often attributed to the force of globalization, but Galtung, in his article "Americanization versus Globalization," argues that the two terms are interchangeable, and the use of "globalization" is only a *façade* to camouflage the real driving force, the Americanization of the Net.[27] Of course, Galtung's argument that "Globalization" is a "code word" for "Americanization" is somewhat dated, given the fact that the

---

[26] Tweedie, Neil, and Thomas Harding. "Diamond Jubilee: The Queen No Longer Rules the Waves." The Telegraph. June 1, 2012. Accessed May 15, 2016. http://www.telegraph.co.uk/news/uknews/the_queens_diamond_jubilee/9305678/Diamond-Jubilee-The-Queen-no-longer-rules-the-waves.html.

[27] Galtung, Johan. "Americanization versus Globalization." In *Identity, Culture, and Globalization*, edited by Eliezer Ben-Rafael, Yitzak Sternberg, and Y. Sternberg, 277-92. Leiden: Brill, 2002, 277.

U.S. is now losing its influence in the global economy. Nonetheless, cyberspace was and has been, to this day, largely dominated by the United States. The Internet was created in and by America and English is, unquestionably, its *lingua franca*: 53.6% of the websites are in English while the second most used language on the Internet, Russian, only accounts for 6.4%.[28] But more importantly, the United States projects its power on cyberspace by manifesting the so-called "hegemonic discourse imperialism."[29] The hegemonic discourse, stripped to its core, is the conscious or unconscious practice of spreading values or ideologies in a way that can manipulate others to adopt the same habit of thoughts. It bears a somewhat close resemblance to Janis' concept of groupthink: A well-established hegemonic discourse encourages a "concurrence-seeking approach" to problems by repressing the contradicting narratives and making them sound like utter nonsense.[30] If managed in a conscious fashion, writes Rusciano, the hegemonic e-narrative can help a country "construct and dominate the descriptions of the world."[31] For instance, when Secretary of State Clinton delivered the speech on Internet Freedom, she actively promoted the "freedoms of digital frontiers in the 21st century," saying, "…those who disrupt the free flow of information in our society or any other pose a threat to [America's] government and civil society."[32] Underlying her remarks is the long-presumed norm regarding the characteristics of cyberspace—that it is a place where values such as freedom of expression or openness, the ethics that founded the U.S. society, should triumph. But by making the features distinctively embedded in American culture the global standards for conduct on cyberspace,

[28] "Usage of Content Languages for Websites." Web Technology Surveys. Accessed May 15, 2016. http://w3techs.com/technologies/overview/content_language/all.
[29] Rusciano, Frank Louis. "The Three Faces of Cyberimperialism." In *Cyberimperialism? Global Relations in the New Electronic Frontier*, edited by Bosah Ebo, 9-26. Wesport: Praeger Publishers, 2001, 11.
[30] Janis, Irving L. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*. 2nd ed. Boston: Houghton Mifflin, 1982.
[31] Rusciano, Frank Louis. "The Three Faces of Cyberimperialism." In *Cyberimperialism? Global Relations in the New Electronic Frontier*, edited by Bosah Ebo, 9-26. Wesport: Praeger Publishers, 2001, 16
[32] Hillary Rodham Clinton, "Remarks on Internet Freedom" (speech, Washington, DC, January 21, 2010), http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

even in places where people hold a completely different view on the issue, is the United States purposefully imposing an imperial uniformity of values upon other countries in cyberspace?

Whether the answer to the above question is "yes" or "no," the fact that the United States has, to some extent, tried to depend on its information advantage to promulgate its ideologies to the rest of the world is irrefutable. In the Information Age, infosphere is a domain that, some experts believe, the United States should strive for dominance:

> For the United States, a central objective of an Information Age foreign policy must be to win the battle of the world's information flows, dominating the airwaves as Great Britain once ruled the seas.
>
> (Rothkopf, David. "In Praise of Cultural Imperialism?" *Foreign Policy* 107 (July 1, 1997): 39. Accessed May 11, 2016. JSTOR Journals.)

But like Britain, "all empires come to an end, and the American one is no exception."[33] The U.S. empire of information is not always welcomed by everybody, and many actors are now demanding the creation of a New International Information Order that is not American-, or Western-, centric.[34] As Mark Twain once reminded us, no country would want "the eagle to put its talon on any other land."[35] The map of information has long been colonized by America; in return, American ideas and practices have shaped the culture of the Internet. But the complex reality of the world cannot be interpreted through the lens of a small elite group. In the end, the construction of cyber discourse should be distributed equally among a variety of actors, not solely controlled by the imperialist bias of a great power.

---

[33] Kyosaki, Robert. *Words of Wisdom: Robert Kiyosaki*, edited by Students' Academy. Lulu Press, 2014.
[34] Cleland, Scott. "The De-Americanization of the Internet." The Daily Caller. November 19, 2013. Accessed May 15, 2016. http://dailycaller.com/2013/11/19/the-de-americanization-of-the-internet/.
[35] Twain, Mark. Mark Twain's Weapons of Satire: Anti-imperialist Writings on the Philippine-American War. Edited by Jim Zwick. Syracuse, NY: Syracuse University Press, 1992, 5.

The Cyber Dragon

During the arduous negotiations of WTO accession terms that began in 1986, a Chinese ambassador was reported to exclaim angrily at the stalemate of the situation, "We know we have to play the game your way now, but in ten years we will set the rules!"[36] Fifteen years after joining the "world's supreme court on trade," China today mesmerizes the international community with her economic prowess; this preoccupation with China's economic growth is reflected in the extensive literature on the rise of China: *The Dragon Awakes*, *The Devouring Dragon*, *China Shakes the World*, *The Rise of the Middle Kingdom*, so on and so forth. As economic capacity is shifting in China's favor, so is military strength. By taking a greater share of global economy, China becomes more influential in redesigning the architecture of the market geography. This change in the spatial distribution of the geoeconomic map sends ripples to the physical geography as well. Beijing's ambition to assert control over the South China Sea and expand its regional influence is no longer a secret. The rise of the East thus poses challenges to the U.S. leadership in both market and physical geographies: The Beijing consensus can become an alternative to the old economic architecture designed by Washington, while China's potential sphere of influence can help consolidate its power and enable it to confront the United States and the West.

In recent decades, the contest for supremacy between United States and China has moved to a new domain—cyberspace. For China, the classic Sun Tzu's philosophy still exerts influence on the country's approach to modern warfare: "To achieve a hundred victories in a hundred battles is not the highest excellence; to subjugate the enemy's army without doing battle is the highest of excellence."[37] This notion of "winning without fighting" directly challenges the age-old Clausewitzian concept of

[36] Chinese ambassador at WTO negotiations, quoted in Christopher A. Ford, China Looks at the West: Identity, Global Ambitions, and the Future of Sino-American Relations (Lexington: University Press of Kentuck, 2015), 394.
[37] Sun, Tzu. "Original The Art of War Translation." Sonshi.com. Accessed May 15, 2016. https://www.sonshi.com/original-the-art-of-war-translation-not-giles.html.

war that "the essence of war is violence."[38] For Sun Tzu, "non-kinetic approach is the pinnacle of war."[39] In a hypothetical armed conflict between the United States and China, it is reasonable to expect that with the advanced military technology, the United States would very well defeat China. "[The Chinese government] has no illusions about its military inferiority *via-à-vis* the United States," writes security analyst Horta, "…as such, [it] has been developing a full range of asymmetric strategies to deter the US until its military reaches maturity."[40] Through the lens of Sun Tzu, the great tactician is the one who always looks for asymmetry in any confrontation and exploits it. Cyber warfare thus exemplifies this concept of asymmetric warfare—where the underdog can take advantage of its superior's weakness and prevail. In the cyber battlefield, the barriers to entry are low, and anyone can learn to develop their own cyber weapons. China's cyber warriors range from the professional hackers trying to disrupt the U.S. information infrastructures to the famous "50-cent Party"—the Internet commentators recruited by the government to spread the party's propaganda. For each pro-government posting, these netizens are reputed to be paid 50 cents of Renminbi.

China has thereby developed its cyber capabilities as the "weapon of the weak" to close the conventional military gap between itself and the United States as well as challenge the U.S. information dominance. Beijing's cyber operations are usually sorted into three categories: "deterrence by paralyzing critical infrastructure, military espionage to gain military knowledge and industrial espionage to gain economic advantage."[41] In 2004, a series of cyber-attacks that began in 2003, commonly known as *Titan Rain*, appeared to have originated from China. Similar attacks persist, and exabytes of data

---

[38] British Admiral Jacky Fisher, quoted in Gary Solis, The Law of Armed Conflict (New York: Cambridge University Press, 2010), 267.
[39] Sun, Tzu. *The Art of War*. Translated by Samuel B. Griffith. Oxford: Oxford University Press, 1963, 77.
[40] Horta, Lorto. "The Dragon's Spear: China's Asymmetric Strategy." The Dragon's Spear: China's Asymmetric Strategy. October 17, 2013. Accessed May 15, 2016. http://yaleglobal.yale.edu/content/dragon's-spear-china's-asymmetric-strategy.
[41] Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (2011): 1-24. Accessed May 15, 2016, 1. doi:http://dx.doi.org/10.5038/1944-0472.4.2.1.

have been carted off by Chinese hackers. Some of the "cyber militias" are state-sponsored with an unclear degree of guidance from the China's People's Liberation Army (PLA) while others only act in China's national interests.[42] Beijing clearly understands that the United States depends heavily on its information system—perhaps more than any other country in the world. Thus, for the United States, defending against these attacks is extremely expensive: "During [the] six-month period the U.S. military alone spent more than $100 million…to remediate attacks on its networks."[43] The costs of cyber espionage can go up to billions of dollars in classified information and intellectual property.[44]

Another contentious issue in Sino-American cyber relations is Chinese widespread resentment toward Western negative coverage of China, especially issues related to Internet censorship. Beijing has a different view on how cyberspace should be run, and China as a whole is not enthusiastic about "[making] the political changes needed to create the liberalism that many in the West are hoping to see in Chinese society."[45] China's Internet censorship practices, usually regarded as a violation of freedom of expression in the United States, seem to not affect Chinese citizens, who, motivated by national loyalty, place the blame on the prejudice embedded in the U.S. and Western media:

> This is a struggle of resistance against western hegemonic discourse. We need to fully recognize that this will be a long-term, difficult and complex battle. But regardless of the outcome, we all firmly believe: western nations' days of using several of their crap media in an absurd attempt to fool people with their rotten words will soon be over for good!
>
> (Original text posted on http://www.anti-cnn.com/index2.html in Chinese [Translation, John Kennedy, Global Voices Online, 24 March 2008) (quoted in Ying Jiang, *Cyber-Nationalism in China. Challenging Western Media Portrayals of Internet Censorship in China*. North Terrace: University of Adelaide, 2012, 8.)

---

[42] Rogin, Josh. "The Top 10 Chinese Cyber Attacks (that We Know Of)." Foreign Policy. January 22, 2010. Accessed May 15, 2016. http://foreignpolicy.com/2010/01/22/the-top-10-chinese-cyber-attacks-that-we-know-of/.
[43] Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011.
[44] Maginnis, Robert. "China Cyber-Stealing Its Way to Super Power Status." Human Events. November 10, 2011. Accessed May 15, 2016. http://humanevents.com/2011/11/10/china-cyberstealing-its-way-to-super-power-status/.
[45] Jiang, Ying. *Cyber-Nationalism in China. Challenging Western Media Portrayals of Internet Censorship in China*. North Terrace: University of Adelaide, 2012, 8.

The political discourse on cyberspace, as argued above, has situated America in a privileged position. But as China is growing in influence, it begins to reclaim the online narrative and resist the inflow of information from the U.S. In the aftermath of the 2008 Tibet riots, Chinese netizens accused Western media of biased coverage of the unrest to tarnish China's image. As an effort to challenge the one-sided rhetoric, young Chinese people registered several anti-Western domains such as: anti-cnn.com, anti-bbc.com, anti-voa.com, etc. The "Century of Humiliation" along with these anti-Western sentiments fueled by media bias eventually become the foundation for Beijing to pursue a more assertive control over cyberspace despite the United States' call for the Internet freedom. But different countries interpret freedom differently. "Freedom is what order is meant for," President Xi Jinping delivers a speech on Chinese version of cyberspace in Wuzhen Internet conference, "and order is the guarantee of freedom."[46] What divides the United States and China over the architecture of the Net is thus value-based: While the United States, fancying itself as a champion for human rights and democracy, advocates for an open cyberspace, China, on the other hand, believes that the internet is only another sovereign space that should be regulated by the PRC. This unmitigated conflict in ideologies seems to have locked both countries into the spiral of "reciprocal demonization" feared by Brzezinski.[47]

Following the aftermath of 2008 financial crisis, Beijing urged the world to become more independent of the volatile Washington: "It is perhaps a good time for the befuddled world to start considering building a de-Americanized world."[48] China is grooming herself as the new leader of this

[46] Kaiman, Jonathan. "What Does 'freedom' Mean? 6 Takeaways from China's Wuzhen Internet Conference." Los Angeles Times. December 16, 2015. Accessed May 15, 2016. http://www.latimes.com/world/asia/la-fg-china-wuzhen-internet-conference-20151216-story.html.
[47] Brzezinski, Zbigniew. "How to Stay Friends With China." The New York Times. January 02, 2011. Accessed May 15, 2016. http://www.nytimes.com/2011/01/03/opinion/03brzezinski.html?_r=0.
[48] Roberts, Dexter. "China's State Press Calls for 'Building a De-Americanized World'" Bloomberg.com. October 14, 2013. Accessed May 15, 2016. http://www.bloomberg.com/news/articles/2013-10-14/chinas-state-press-calls-for-building-a-de-americanized-world.

global *coup d'état* against the dominance of the United States. Committed to asserting her own place in the physical, market, and now, information, geography, Beijing is overturning the geopolitical equation of the world. Against America's wish, the Dragon is ready to write its own rules.

Information-Industrial Complex

Back in 1961, President Eisenhower warned the public about the hazard of the military-industrial complex as a "disastrous rise of misplaced power."[49] In the Information Age, however, we are witnessing what Powers and Jablonski describe as the "information-industrial complex,"[50] a term reflecting the growth of the information technology sector as a more influential player in Washington. Given that the Internet has been substantially privatized and users now choose to concentrate on corporate-owned platforms, most of the online data are now on the servers of high-tech companies such as Facebook, Google, Apple, Microsoft, and so on. It is thus reasonable to expect that these corporations, knowing how to capitalize on the information of their userbase, start to play a larger role in the discussion over cyber-related issues. But like the military-industrial complex, the information-industrial complex can be "an ineffective model for the governments and the businesses alike."[51] When cyberspace is a locus of international politics, the Internet tycoons, like other entities in the realm of global affairs, pursue their own interests, and in many cases, the interests of these corporate powers do not align with those of the U.S. government. This tension between the principles embraced by digital corporations and the national security goals that the U.S. government wants to accomplish can eventually culminate in the declining influence of American statecraft and diplomacy.

[49] Eisenhower. "Military-Industrial Complex Speech." 1961.
[50] Powers, Shawn M., and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana: University of Illinois Press, 2015, 50.
[51] Ibid., 51.

The recent "encryption battle" between the FBI and Apple, widely known as the "Apple Test Case," perfectly illuminates the current debate between digital privacy and national security concerns in contemporary American politics. After the San Bernardino attack last year, the U.S. District court of California issued an order asking Apple to unlock the cellphone used by one of the shooters. Specifically, Apple was required to design an entirely new operating system that would allow the FBI to *brute force* attack the phone without wiping the data. The United States government believed that by hacking the gunman's iPhone, they could obtain useful information that could help prevent another terrorist attack. The problem is, once a system to break encryption is created in the digital world, it cannot be destroyed and can become an awful tool when fallen into the wrong hands. Unlocking one would mean unlocking all. CEO Tim Cook quickly sent a letter to all Apple employees, calling the demand from the government "a terrible idea" and "a dangerous precedent that threatens civil liberties."[52] This struggle between U.S. national security establishment and Apple's protocols to protect users' privacy underscores many of the existing dilemmas of the relationship between U.S. government and corporations in Information era: Information technology is at once a powerful advantage of the U.S. government, but it has also empowered the private sector to resist government regulations and control. The Apple Test Case, however, sets an unprecedented publicity of tech-civil disobedience that only further complicates Apple's relationship with the White House.

The power of Silicon Valley giants has also extended into the diplomatic realm. In 2015, during President Xi's first state visit in the United States, his first stop was not Washington, but Seattle. His order of visits understandably surprised many people; however, the fact that Internet companies are now filling the "diplomacy vacuum" left by the U.S. government is not a new trend.[53] Indeed, a lot of

[52] Cook, Tim. "Read the Letter Tim Cook Wrote to Apple Employees Today." MarketWatch. February 22, 2016. Accessed May 15, 2016. http://www.marketwatch.com/story/read-the-letter-tim-cook-wrote-to-apple-employees-today-2016-02-22.

[53] Liao, Rebecca. "Digital Diplomacy." Foreign Affairs. October 12, 2015. Accessed May 15, 2016. https://www.foreignaffairs.com/articles/china/2015-10-12/digital-diplomacy.

tech giants have taken on state-like behavior and used their diplomacy card. The concept of "Silicon Valley Diplomacy," referring to the development of foreign policy aspect in corporations' strategy, has been around for quite some time. Facebook is one of the companies that have overtly attempted at diplomatically engaging with foreign governments. Zuckerberg has hired his own team of ambassadors, people who are "comfortable with politicians at the most senior levels of government," in order to promote Facebook interests abroad.[54] The company's long-sought target for market, until this day, remains China. Since Facebook was blocked in China nine years ago, the young CEO has tried to curry favor with the PRC in the hope of re-entering the market. He has been learning to speak fluent Mandarin Chinese and courting many Chinese politicians and entrepreneurs over the years. His popularity among Chinese populace thus quickly pumped up,[55] although his ambitious plan to charm the Chinese government into letting his company get access to a third of the world's population had little success. In 2011, Zuckerberg was quoted saying, "I don't want Facebook to be an American company… I don't want it to be this company that just spreads American values all across the world."[56] Alienating his company from the common rhetoric of the U.S. government, Zuckerberg has established Facebook as an independent entity largely motivated by corporate, not American, interests.

Information Spring

> "The 21st century is a terrible time to be a control freak."
>
> —Alec Ross, *The Industries of the Future* (New York: Simon and Schuste, 2016), 186.

The *Guardian* was the first to publish the leak of classified National Security Agency (NSA) documents. The identity of the whistleblower was later revealed, at his request. A patriot to some, a

[54] Estes, Adam Clark. "Signs That Facebook Is Acting Like a Sovereign Nation." The Wire. May 24, 2011. Accessed May 16, 2016. http://www.thewire.com/technology/2011/05/signs-facebook-acting-like-sovereign-nation/38103/.
[55] Florcruz, Michelle. "Mark Zuckerberg Is Not Fluent In Mandarin Chinese, But It Is Still Impressive." International Business Times. October 23, 2014. Accessed May 16, 2016. http://www.ibtimes.com/mark-zuckerberg-not-fluent-mandarin-chinese-it-still-impressive-1711480.
[56] Mark Zuckerberg quoted in John Boudreau, Culture clash at heart of Facebook's China problem, available at http://www.siliconvalley.com/sv2020/ci_18450897?%20%20source=rss

traitor to others—whatever your perception of Edward Snowden might be, it does not change the fact that the 32-year-old is now an international phenomenon as the individual responsible for one of the biggest information breaches in history. Just days after his revelations, the sales of George Orwell's dystopian classic, *1984*, spiked by 6000 percent.[57] According to the leaked documents, the NSA's surveillance system monitored the private lives of many innocent Americans, which made the agency dangerously resemble Big Brother, the authoritarian leader of Orwell's Oceania. The public backlash against NSA followed shortly after: The "Restore the Fourth (Amendment)" movement attracted thousands of supporters; in San Francisco, anti-NSA protestors, wearing Snowden masks, rallied across the city and demanded the government to shut down the surveillance program.[58] Snowden's leaked information about NSA's covert surveillance apparatus triggers a debate on who owns information and what type of information should be brought to light. It is the imprint of the Information Age, when information is now at the center of the political struggle. States do not have the monopoly on information anymore: information flows from top to bottom, from governments to corporations, and now, to the people. The disclosure of NSA's secret information empowers ordinary American citizens to defy their government, and Snowden himself warned of a "shift in balance of power" that is driven by "an informed public."[59] A revolution is unfolding—a moment of power transfer, a point of civil defiance, a demand to know, an Information Spring that will surely challenge the authority of the power elite.

---

[57] Kim, Eun Kyung. "Sales of Orwell's '1984' up over 6,000 Percent after NSA News." TODAY.com. June 11, 2013. Accessed May 16, 2016. http://www.today.com/news/sales-orwells-1984-over-6-000-percent-after-nsa-news-6C10282307.

[58] Bowe, Rebecca. "NSA Surveillance: Protesters Stage Restore the Fourth Rallies across US." The Guardian. July 05, 2013. Accessed May 16, 2016. http://www.theguardian.com/world/2013/jul/04/restore-the-fourth-protesters-nsa-surveillance.

[59] Ratcliffe, Rebecca. "Snowden: balance of power has shifted as people defy government surveillance." The Guardian. July 04, 2015. Accessed May 16, 2016. http://www.theguardian.com/us-news/2015/jun/05/snowden-balance-power-shifted-people-defy-government-surveillance-nsa

The Information Spring in the United States, however, should not be unanticipated. Back in 1971, military analyst Daniel Ellsberg released seven thousand pages on Department of Defense's analytical record of American involvement in the Vietnam War, usually referred to as the Pentagon Papers. The *Times* published excerpts from the documents, revealing that the U.S government, from Truman to Johnson administration, deliberately lied about its conduct in the Vietnam War. After 9/11, William Binney, along with three former NSA officials, exposed the wrongdoing of the organization's Trailblazer program, calling it the "largest failure in NSA history."[60] "Keeping secret is not an easy task," Schoenfeld laments, "because Washington leaks like a sieve."[61]

From a historical point of view, Snowden's leak of top-secret documents is thus not unprecedented; nevertheless, it is the turning point for the Information Spring because the technology of the Information Age has enabled Snowden to pull off one of the most spectacular thefts of all time. Managing to disguise himself as a "ghost user" on cyberspace, he skillfully exploited the hole in the NSA's antiquated system and got access to the vast information of NSAnet without leaving a trace.[62] This is truly remarkable, especially compared to how Ellsberg obtained the Pentagon Papers 45 years ago: He was a part of the team that worked on the study in 1967, and when deciding to publish the documents two years later, he had to spend several weeks copying the report. Moreover, given the ubiquity of the Internet, Snowden's highly classified documents spread like wildfire. The large scale of his data-set revealed that the White House was not only spying on its citizens but also on its allies. The allegation that the U.S. government eavesdropped Chancellor Merkel's phone had strained the Amertican-German relationship and raised doubt about the trustworthiness of the United States.

---

[60] William Binney quoted in Zack Whittaker, Drowned in data, whistleblowers speak of NSA's "largest failure", available at http://www.zdnet.com/article/nsa-whistleblowers-security-thinthread-largest-failure-in-nsa-history/

[61] Schoenfeld, Gabriel. "Rethinking the Pentagon Papers." National Affairs, no. 4 (Summer 2010). Accessed May 16, 2016. http://www.nationalaffairs.com/publications/detail/rethinking-the-pentagon-papers.

[62] Esposito, Richard, and Matthew Cole. "How Snowden Did It." NBC News. August 26, 2013. Accessed May 16, 2016. http://www.nbcnews.com/news/other/how-snowden-did-it-f8C11003160.

The momentum of the Information Spring continued three years later. On April 3, 2016, the international community witnessed the biggest data-drop to date: 11.5 million documents, or 2.6 terabytes of data, were leaked from Mossack Fonseca, a Panama-based law firm, to German newspaper *Süddeutsche Zeitung*. The so-called Panama Papers implied that law firms helped the powerful and wealthy people launder money and avoid taxes. Through Mossack Fonseca, the "rich and famous" established offshore shell companies in Panama, one of the most well-known tax havens. The impact of the so-called Panama Papers was immediately felt around the world: Within 48 hours of the leak, Iceland Prime Minister was forced to step down by his people and the opposition party. The public outcry spread to England after Cameron's father was revealed to have set up an offshore company in Panama. Calls for the PM's resignation quickly escalated. Of course, in other parts of the world, the documents were handled differently: The associates and relatives of Putin and Xi are involved in the scandal; as a response, China blocked all the information related to the Panama Papers[63], while Russia dismissed it as another plot from the West to fuel "Putinophobia."[64] However, despite successfully quelling opposition, both Russia and China cannot resist the movement of the people for long. To avoid the censorship, many Chinese users now share screenshots on the news, making it harder for the sensors to identify the keywords.[65] The information from Panama Papers enraged the public throughout the globe and illuminated how the political establishment had worked only for the wealthiest. Panama leak continued to nourish public resentment towards the secrecy of the elites and encourage other massive disclosures of information to follow.

[63] Porzucki, Nina. "Censors in China: 'What Panama Papers?'" Public Radio International. April 7, 2016. Accessed May 16, 2016. http://www.pri.org/stories/2016-04-07/censors-china-what-panama-papers.
[64] Luhn, Alec, and Luke Harding. "Putin Dismisses Panama Papers as an Attempt to Destabilise Russia." The Guardian. April 07, 2016. Accessed May 16, 2016. http://www.theguardian.com/news/2016/apr/07/putin-dismisses-panama-papers-as-an-attempt-to-destabilise-russia
[65] Porzucki, Nina. "Censors in China: 'What Panama Papers?'" Public Radio International. April 7, 2016. Accessed May 16, 2016. http://www.pri.org/stories/2016-04-07/censors-china-what-panama-papers

During a press conference in Arizona, Secretary of Defense Donald Rumsfeld spoke to the public, "Our country has forgotten how to keep a secret."[66] For a long time, diplomacy has always been guarded by the veil of secrecy, but the tide of Information Spring has reinforced renewed demand for more government transparency. Information disclosure, especially disclosure of classified national security secrets, becomes the norm, and information gives people the power they could never have in the past. Emboldened by the data leaks, the public can now confront their governments and hold them accountable for their wrongdoings. For the United States, striking the balance between transparency and security is harder than ever: State secrecy can poison democracy, but openness can endanger security. Theoretically, a harmony between the two elements would be healthy for U.S. leadership, but deluding ourselves into believing that such a balance exists is wistful thinking. The Unites States is in the midst of a revolution, and the Information Spring is tipping the balance of power in favor of the people, for "Until they become conscious they will never rebel."[67] More Snowdens will emerge, and citizens will have more access to change policies. It is a bitter, yet necessary, pill to swallow: The United States has no choice but to live with the leak culture, although it means that the President has less room to maneuver when it comes to security. The only way to mitigate the effect of the Information Spring is to remind people of their need for national security, and that need will sometimes have to eclipse their pledges for transparency.

[66] Donald H. Rumsfeld, "Comments at Secretary Rumsfeld Press Conference" (speech, Phoenix, Arizona, August 26, 2004), http://www.fas.org/sgp/news/2004/08/dod082604.html
[67] Orwell, George. "Chapter 7." In 1984, by George Orwell. EBooks@Adelaide. Accessed May 16, 2016. https://ebooks.adelaide.edu.au/o/orwell/george/o79n/chapter1.7.html.

PART C: "Putting the 'I' back into DIME"

The Information Age is in full swing: In 1900, human knowledge doubled every 100 years. In 2013, it doubled every 13 years. In 2020, it is predicted to double every 12 hours.[68] As information technology becomes the primary vector of global growth, individuals now have the ability to obtain and control information at speeds and in volumes that people in the past would have never found fathomable. But when information changes hands, power changes hands. The rapid dissemination of information is thus rocking the power structure of the world in a way we have never seen before. Information security, as a result, takes on new prominence. Geoinformation emerges as a new geopolitical branch that shines the spotlight on the significance of information as a resource of power and drives the formulation of grand strategy in the Information Age. Nonetheless, the conviction that the information revolution will make the "tyranny of geography" fade away does not take into account a new domain central to geoinformational calculations. Cyberspace, a sub-region of infosphere, has pervaded more deeply into the function of modern societies. Alive with information, this virtual space is bridging borders and allows its inhabitants to get access to a wide array of information across the globe. Although cyberspace is generally a non-physical terrain, the rise of cyberspace does not mean a collapse of materiality or the death of geography. On the contrary, a true great power must learn to control the three spaces of the world: the physical, market and information geography.

Cyberspace, as the hub of most digital information, is now the strategic domain in its own right. But it was never born neutral. Funded by the U.S. Department of Defense, the Advanced Research Projects Agency Network (ARPANET) laid the first technical foundation for the Internet. As a result, the United States has long dominated the cyber-discourse that digitally export American

[68] Schilling, David Russell. "Knowledge Doubling Every 12 Months, Soon to Be Every 12 Hours - Industry Tap." Industry Tap. April 19, 2013. Accessed May 16, 2016. http://www.industrytap.com/knowledge-doubling-every-12-months-soon-to-be-every-12-hours/3950

ideas, values and world visions. But its status as the information empire is consistently challenged; the call to "de-Americanize the Internet" unsurprisingly attracts a lot of supporters in the international community.[69] China, of course, does not squander this opportunity to join the movement and push back against the U.S.'s one-way control of the Internet governance. Moreover, the Internet giants, albeit established in the U.S., also gain their fair share in the distribution of cyberspace and pursue their independent diplomatic goals. Some of those corporations deliberately disassociate themselves from the government and only focus on advancing their interests abroad, sometimes at the expense of American interests. Last but not least, informed citizenry is now on the road to confrontation with their government over national security secrets. Recent disclosures of the government's clandestine activities leads to the public outrage that starts the Information Spring. The movement is global in nature, although in the short run, it will affect democracies more than authoritarian states.

Moving forward, the United States needs to account for these challenges in the formulation of national security strategy and reclaim her place in the map of information. A geoinformation-based framework should include three pillars, namely, (1) an agreement on the Internet governance and cybersecurity with China, (2) greater cooperation with Silicon Valley based on common interests, and (3) cautious management of the Information Spring. To execute (1) and (2), the United States has to acknowledge that the heyday of her information empire has come to an end and let other actors participate in shaping the contour of information map. The U.S. still enjoys certain advantages nonetheless, given how she contributes to the infrastructure of Internet we see today.

The last pillar, cautious management of the Information Spring, is critical for the United States, for the better the America handles the revolution, the more likely the pendulum will swing back in her favor. In the long run, the Information Spring will give all citizens the tools necessary to build their

[69] Cleland, Scott. "The De-Americanization of the Internet." The Daily Caller. November 19, 2013. Accessed May 15, 2016. http://dailycaller.com/2013/11/19/the-de-americanization-of-the-internet/.

own sources of power. Authoritarian states will try to block the flows of information, but information is not something that can be contained. It can move across borders in various forms, even under the government's closest surveillance. The monopoly of authoritarian regimes on information will eventually become intolerable for their citizens, and those regimes will have to either be more transparent about their activities or confront an inevitable people's revolution that can topple down the regimes. In either of these cases, the United States is assured to have more leverage to influence global outcomes. But for now, until the Information Spring comes in full force, America has to bide her time and wait. In the end, the Information Age has changed our world profoundly and irreversibly, but "it is unlikely that the information age will be as good as we hope or as bad as we fear. It will certainly be far different than we imagine."[70]

[70] Wresch, William. *Disconnected: Haves and Have-nots in the Information Age*. New Brunswick: Rutgers University Press, 1996, 247.

BIBLIOGRAPHY

Barlow, John Perry. "A Declaration of the Independence of Cyberspace." *New Internationalist*, no. 479 (January 1996: 27.

Boulding, Kenneth E. *Three Faces of Power*. Newbury Park, CA: Sage Publications, 1989.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011.

Choucri, Nazli. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press, 2012.

Dahl, Robert. "The Concept of Power." *Behavioral Science* 2, no. 3 (1957), 201-215.

Friedman, Thomas L. *The Lexus and The Olive Tree: Understanding Globalization*. 1st ed. New York: Farrar, Straus, Giroux, 1999.

Galtung, Johan. "Americanization versus Globalization." In *Identity, Culture, and Globalization*, edited by Eliezer Ben-Rafael, Yitzak Sternberg, and Y. Sternberg, 277-92. Leiden: Brill, 2002.

Gibson, William. *Neuromancer*. 1st ed. Ace, 1984.

Granieri, Ronald J. "What Is Geopolitics and Why Does It Matter?" *Orbis* 59, no. 4 (2015): 491-504. Accessed April 20, 2016. doi:10.1016/j.orbis.2015.08.003

Hartshorne, Richard. "Political Geography." In *American Geography: Inventory and Prospect*, edited by P. James and C. Jones, 211-14. Syracuse, NY: Syracuse University Press, 1954.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (2011): 1-24. Accessed May 15, 2016. doi:http://dx.doi.org/10.5038/1944-0472.4.2.1.

Janis, Irving L. Groupthink: *Psychological Studies of Policy Decisions and Fiascoes*. 2nd ed. Boston: Houghton Mifflin, 1982.

Jiang, Ying. *Cyber-Nationalism in China. Challenging Western Media Portrayals of Internet Censorship in China.* North Terrace: University of Adelaide, 2012

Kyosaki, Robert. *Words of Wisdom: Robert Kiyosaki*, edited by Students' Academy. Lulu Press, 2014

Li, Sheng. "When Does Internet Denial Trigger the Right of Armed Self-Defense?" *Yale Journal of International Law* 38, no. 1 (2013): 179-216. Accessed May 15, 2016. http://ssrn.com/abstract=2226793.

Liao, Rebecca. "Digital Diplomacy." Foreign Affairs. October 12, 2015. Accessed May 15, 2016. https://www.foreignaffairs.com/articles/china/2015-10-12/digital-diplomacy.

Lundborg, Tom. "What Lies Beyond Lies Within: Global Information Flows and the Politics of the State/Inter-State System." *Alternatives: Global, Local, Political* 36, no. 2 (May 2011): 103 – 117.

Mackinder, H. J. "The Geographical Pivot of History." *The Geographical Journal* 23, no. 4 (April 1904): 421-37. doi:10.2307/1775498

McDowell, Stephen D., Philip E. Steinberg, and Tami K. Tomasello. *Managing the Infosphere: Governance, Technology, and Cultural Practice in Motion*. Philadelphia: Temple University Press, 2008.

Powers, Shawn M., and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana: University of Illinois Press, 2015.

Ross, Alec. *The Industries of the Future*. New York: Simon and Schuste, 2016.

Rusciano, Frank Louis. "The Three Faces of Cyberimperialism." In *Cyberimperialism? Global Relations in the New Electronic Frontier*, edited by Bosah Ebo, 9-26. Wesport: Praeger Publishers, 2001.

Schaap, Arie J. "Cyber Warfare Operations: Development and Use Under International Law." *Air Force Law Review* 64 (2009): 121-74.

Schoenfeld, Gabriel. "Rethinking the Pentagon Papers." National Affairs, no. 4 (Summer 2010). Accessed May 16, 2016. http://www.nationalaffairs.com/publications/detail/rethinking-the-pentagon-papers

Silver, Daniel B. "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter." Edited by Michael N. Schmitt and Brian T. O'Donnell. *Computer Network Attack and International Law* 76 (2002): 90-91.

Sun, Tzu. *The Art of War*. Translated by Samuel B. Griffith. Oxford: Oxford University Press, 1963

Spykman, Nicholas J. "Geography and Foreign Policy, II." *The American Political Science Review* 32, no. 2 (April 1938): 213-236.

Tuathail, Gearoid O., and Simon Dalby. *Rethinking Geopolitics: Towards a Critical Geopolitics*. New York: Routledge, 2002.

Twain, Mark. *Mark Twain's Weapons of Satire: Anti-imperialist Writings on the Philippine-American War*. Edited by Jim Zwick. Syracuse, NY: Syracuse University Press, 1992.

Wresch, William. Disconnected: Haves and Have-nots in the Information Age. New Brunswick: Rutgers University Press, 1996.