A Prime Directive: Placing Agendas for Cyberspace in Perspective

Chris Bronk

Rice University

Paper submitted to the 54th Annual Convention of the International Studies Association, April 3-6, 2013

"Anything you dream is fiction, and anything you accomplish is science, the whole history of mankind is nothing but science fiction. "

Ray Bradbury

On July 21, 2011 the Space Shuttle Orbiter *Atlantis* completed her final mission into low-earth orbit, some thirty years after the United States initiated the program. *Atlantis* took with her the final major pieces necessary for completion of the International Space Station (ISS). And with her landing at the Kennedy Space Center, the United States government's capacity to launch and recover its astronauts came to an abrupt end. Weeks after, China launched its first experimental space station into orbit, a testbed for orbital docking missions with its Shenzhou spacecraft. NASA was humiliatingly left without an American successor. Anything going to or from the ISS would need to ride on a Russian Soyuz spacecraft launched from the former Soviet Cosmodrome at Baikonur, Kazakhstan.

And then Silicon Valley entered the picture. Little more than a year after the last shuttle flight, a rocket again blasted off from Cape Canaveral with the ISS as its payload's destination. Aboard it was a Dragon space capsule, a vehicle not operated by NASA, but instead by SpaceX, a company founded by Elon Musk, an information technology entrepreneur best known for his role in the creation of PayPal, an electronic payment system geared for Internet-based transactions. Dragon successfully docked with the ISS and splashed down back on Earth with only minor hiccups. The mission was billed as a success for Silicon Valley, free markets, and

American innovation. America's Internet billionaires, many of them immigrants, could be the new stewards of the nation's destiny in outer space.

The "Valley saves NASA" narrative is yet another triumph of the Internet-computing innovation complex in the United States. Elon Musk's future ventures, in not only space, but electric cars and solar power, once might have been laughed off as the hobbies of an eccentric, if my hardcore geek colleagues weren't buying those cars sight unseen with a wait that rivals that of Aston Martin. But this Internet triumphalism has its detractors. It is an outgrowth of the *solutionist* agenda described by Evgeny Morozov found in the Valley – the idea that with enough data and smarts, almost any problem may be licked.[1] There is much to admire about Morozov's critique of the shiny Californian view of better living through big data mindset, but as my colleague Mary Joyce wondered, is it possible to get past cyber–optimism and –pessimism?

That question I will leave to others, instead, I want to consider how fiction of our possible future or other worlds and times – science fiction – frames the international politics of our present, a time marked by massive networked computerization. While we can debate the centrality of the Internet in contemporary international politics, the proliferation of devices employing Internet Protocol to communicate with one another is remarkable. That packetized IP-based

---

[1] Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism*, PublicAffairs: New York, 2013.

communication is now so much of the world's communication volume – web pages served, emails delivered, Skype sessions connected, tweets delivered – is remarkable. Rail gauge differences may require a change of trains from one country to another, and the world has two standards for electricity, but IP has become the dominant transmission and delivery mechanism for data between computers. We are interlinked, and that linkage is a new venue for international relations that often involves hardly a nation at all.

At root here is the question of whether the creation of cyberspace – computer networks that make communication increasingly simple and rich over distance – is making the world more or less prone to conflict.[2] There are other questions as well, for instance does cyber conflict mean a competition of ideas, the theft of them, or the doomsday scenarios who wish to place the term cyber in front of any bad prior event (although nobody is yet asking us to "Remember the [cyber] Maine"). There is a general sentiment that a certain degree of utopianism once existed regarding cyberspace, but now that thinking is being replaced by some very hard cyber politics. But as Nye reminds us, "Power depends on context, and cyber power depends on the resources that characterize the domain of cyberspace."[3] Understanding the context of power relationships allows us to better consider what the future of conflict that incorporates cyberspace as one of its elements.

---

[2] See Mary Manjikian, "From Global Village to Virtual Battlespace: the Colonizing of the Internet and the Extension of Realpolitik." December 2010. *International Studies Quarterly*.
[3] Joseph Nye, *Cyber Power*, Belfer Center for Science and International Affairs, May 2010, p. 3.

"So the whole war is because we can't talk to each other."

Orson Scott Card, *Ender's Game*

The germ from which this essay sprang was a class discussion regarding Orson Scott Card's 1985 novel *Ender's Game*. For those not familiar with *Ender*, it is one of the most significant works of science fiction in the last generation. Its hero-protagonist, a brilliant youth, Ender Wiggin, is selected for military leadership training to combat an existential threat posed by a sophisticated and ruthless enemy. Ender and his classmates learn through games and simulation until it is revealed in the book's major twist of plot that the simulations have long been over and the virtual campaign undertaken from a hidden command center is very real and decisive. Ender sends millions of fellow humans to their deaths in a struggle that likely exterminates the enemy.

This should remind IR theorists of James Der Derian's work following the 1991 Persian Gulf War,[4] a conflict greatly sanitized by the Department of Defense for media consumption and carrying with it an almost absurdly lopsided casualty count. So despite Morozov's caution, I must again suggest that we are in the midst of something of a major change in human organization, sovereignty and conflict due to innovation particularly in the area of computing. I will offer nothing more on outer

[4] Consider: James Der Derian, "The Simulation Syndrome: From War Games to Game Wars", *Social Text*, Spring1990.

space, but instead only consider cyberspace, and my reading of science fiction, some of which pertains to outer space, as it applies to cyberspace.

Several books framed my thinking on this paper, including Frank Herbert's *Dune*, William Gibson's *Neuromancer*, and perhaps most importantly the original trilogy of Isaac Asimov's *Foundation*. Science fiction, from Star Trek and Star Wars to the writings of the authors above as well as other luminaries including Ray Bradbury, Arthur C. Clarke, Philip K. Dick, and H. G. Wells have done much to shape the common consciousness of American computer technologists. They provide images, metaphors and alternate views of technology, politics and human interaction that may be of utility in thinking about how an increasingly computerized and interconnected world will look and how it can be safely managed.

"Politicians should read science fiction, not westerns or detective stories."
Arthur C. Clarke

As cyber issues become a more significant element of geopolitics, they attract more attention from policymakers. Today, those in positions of economic and political leadership are concerned for or with cyberspace. The crime, espionage, and warfare connected to the term cyber are widely discussed, but it was not long ago that one U.S. elected official was widely lampooned for describing the Internet as "a series of tubes," seemingly unaware of how the metaphor applied.

For the last 20 years, governments around the world have largely left the Internet, the key technical infrastructure of cyberspace, alone, often providing subsidies and investment without heaping on regulation or taxation. The cyber attacks against Estonia in 2007, the Wikileaks episode, the digital components of the Arab Spring revolutions, and the Stuxnet campaign against the Iranian nuclear enrichment program each stand as markers in drawing the attention of the powerful beyond those in the technology industry itself. Microsoft founder Bill Gates recently argued at a conference in Houston, "Cyber security has been an issue for the last decade or so. But it's getting more attention now and it should be getting more because it's just now – or should be this way – being looked at in geopolitical terms."[5]

The international politics crowd occasionally convenes to consider cyberspace, the Internet, and information technology (IT). Last decade, it was the World Summit on the Information Society (WSIS) in Tunis. Last year, it was the World Congress on Information Technology (WCIT). Both these assemblies were largely cast as debates on the role of the United States in governing the Internet. But this presupposes that the government of the United States, or any government, has the capacity to completely assert its will on how the Internet is run, or indeed how it was ever constructed in the first place.

What the U.S. delegation to WCIT argued, apparently in a persuasive manner, was that governance of the Internet, the technical construct underpinning the rhetorical

---

[5] Bill Gates, CeraWeek Address, Houston, TX, March 7, 2013.

one called cyberspace, is best left to a multi-stakeholder arrangement. Government agencies have a role in this, but so does industry, and with it the assortment of technologists charged with making the Internet run (plus the catchall civil society has a role).

The engineers of the Internet did not bring it to the massive audience it enjoys, the profit motive did. Nonetheless, without a clique of engineers, cyberspace would not be. The technologists are very much a part of the politics of cyberspace, but it is difficult to determine what power they hold.

"I'm going to watch our screens and try to see a Guildsman."
"You won't. Not even their agents ever see a Guildsman. The Guild's as jealous of its privacy as it is of its monopoly. Don't do anything to endanger our shipping privileges, Paul."
Frank Herbert - *Dune*

In *Dune,* the elder Atreidis passed the wisdom to his son regarding the enormous power of the Spacing Guild holding the interstellar travel monopoly. This guild is a useful metaphor. In 2011, at the inaugural Cyber Dialogue, Paul Twomey reminded us that the people who make the Internet function, those technicians and engineers of routers, switches, and other logical devices stand as a guild.[6] And what might he

[6] Paul Twomey, Cyber Dialogue, 2011, http://www.cyberdialogue.ca/previous-dialogues/2011-about/

mean? A fairly standard definition of a guild is an association of artisans; people who make things. Guilds grew up in medieval Europe, passing knowledge from generation to generation. They occupied a precarious space between the feudal elite and the mass of peasantry eking out subsistence from the land and underwriting the needs of the nobility, who offered martial protection in exchange for taxes. While the peasants toiled and the lords protected, the guilds built modernity.

But in thinking of cyberspace, it is worthwhile to think of how the guild that makes the Internet run came to be.[7] The Internet grew up around a rather unusual entity, the Internet Engineering Task Force (IETF), in roughly a generation. These engineers created new pieces of functionality, maintained the infrastructure needed to route an unfathomable number of messages, and managed the Internet's phenomenal growth. Without this technological guild, the Internet would not work, but how does it exert power and how much of it does it have?

We can get an idea of this from the swift and persistent response to the 2011 Stop Online Privacy Act (SOPA) and the Protect IP Act (PIPA) legislative initiatives in the U.S. Congress. As written, both bills would have essentially banned the fruit of 20 years' effort to develop the Internet Protocol Security (IPSec) protocol suite.[8] The SOPA/PIPA lesson was clear. Governments could attempt to exert control over

---

[7] Barry Leiner et. al., *Brief History of the Internet,* http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

[8] In response, I did what academics typically do, writing an op-ed piece and signing a petition probably the only time my name will appear anywhere near both Peter Gabriel and Glenn Beck's.

cyberspace, but if enough interested parties who make it work disagreed, government's capacity to control it could be fairly effectively thwarted. Unfortunately cyberspace is also a convenient avenue for those with the requisite skills to penetrate corporate, government, and organizational networks and purloin information, thus disrupting it.

"[J]acked into a custom cyberspace deck that projected his disembodied consciousness into the consensual hallucination that was the matrix. A thief, he'd worked for other, wealthier thieves, employers who provided exotic software required to penetrate the bright walls of corporate systems, opening windows into rich fields of data."
William Gibson - *Neuromancer*

The news often portrays that all hell has broken loose in cyberspace. Indeed, cyberspace is increasingly becoming a venue for conflict between parties – states, transnational groups, corporations, political movements, and others. There is new power to be found in cyberspace, an area the U.S. Department of Defense labels a domain of conflict and a place where it plans to send thousands of its soldiers, sailors and airmen to do battle. One journalist reports that 12 of the 15 largest military powers have active cyber warfare programs,[9] but military doctrinaires still leave most of us wondering what cyberwar is or isn't.

---

[9] Richard Sale, "Cyber War Stakes Rising," *ISS Source*, January 9, 2013, http://www.isssource.com/cyber-war-stakes-rising/

Luckily we still reside at a point where rhetoric goes far beyond reality in cyber warfare. Much of what makes headlines is actually espionage undertaken by cyber means. In its recent report, American cybersecurity firm Mandiant produced an extraordinarily detailed view of cyber espionage activities being undertaken from China.[10] But what was remarkable about the company's research was their ability to unequivocally argue that, "The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them."

China has developed a massive cyber intelligence capability designed to purloin the intellectual products of foreign firms and enable the rapid technological advancement of its state-run industries and research institutions. It is not China alone engaging in cyber espionage, as the U.S. Office of the National Counterintelligence Executive (ONCIX) stated in its 2011 report, "Certain allies and other countries that enjoy broad access to US Government agencies and the private sector conduct economic espionage to acquire sensitive US information and technologies. Some of these states have advanced cyber capabilities." [11] Being fair, the PRC accuses the United States of making more than 100,000 attacks a month upon its websites.[12]

---

[10] Manidant, *APT1: Exposing one of China's Cyber Espionage Units*, 2013, http://intelreport.mandiant.com/

[11] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage*, 2009-2011, October 2011, p. i.

[12] Leo Lewis, "Beijing claims US is making 100,000 cyber-attacks a month," *The Times*, March 1, 2013.

The imagined world of widespread cyber espionage from Gibson's *Neuromancer* is now very real. Globally interconnected, multinational corporations remain big, ripe targets. As my colleague Dan Wallach commented on the Mandiant report, with regard to the Chinese hackers of its Unit 61938, "I'm most taken aback by the lack of sophistication and poor tradecraft."[13] This should resonate with corporate and government leaders alike – the Chinese hackers who've perpetrated what has been called (fairly or not) the greatest transfer of wealth in human history[14] have achieved incredible results with mediocre effort. But cyber espionage is being eclipsed. The capacity to turn on and off machines, damage industrial plant, and possibly even endanger human life via cyber means is no longer conjecture, but rather a real possibility.

"Violence is the last refuge of the incompetent."
Isaac Asimov, *Foundation*

Cyberspace has transformed the practice of intelligence, but may also usher in a new golden age in covert action. *Stuxnet* demonstrated a crossing of the Rubicon in cyber covert action designed to impact computer-controlled physical infrastructure. To anyone who finds appeal in John Perry Barlow's "A Declaration of the

---

[13] Correspondence with author, March 11, 2013.
[14] Josh Rogin, "NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history," *Foreign Policy*, July 9, 2012, http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history?wp_login_redirect=0

Independence Cyberspace,"[15] the use of cyberspace as a mechanism for clandestine military attack is revolting. To Barlow, cyberspace wasn't supposed to be a venue for conflict, it was supposed to be, "a civilization of the mind…more humane and fair than the world your governments have made before."

Sadly, this is not the case. Cyberspace is becoming a battlefield, in which the lines between soft and hard power blur. I opined on the current state of affairs in cyber conflict recently. Of cyber attacks, I argued:

> As long as they work, countries and plenty of others will launch cyber-attacks that blur the differentiation between power of persuasion and hard coercive force in combinations of diplomacy, trade, covert action and military intervention. A friend suggested a term for placement of cyber-action across the spectrum of international affairs: shoft (mostly soft, but with some hard elements). Most soft U.S. cyberpower is in Silicon Valley. But there is a growing area of cyber-action with physical ramifications in other places -- see Stuxnet and Shamoon.[16]

Like the land, seas, and skies before, military forces are now considering how to make this human constructed commons, cyberspace, a productive avenue for

---

[15] John Perry Barlow, "A Declaration of Independence of Cyberspace," https://projects.eff.org/~barlow/Declaration-Final.html

[16] Chris Bronk, "Hacking Isn't Cyberwar, for Now, New York Times, February 28, 2013, http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/hacking-is-hardly-cyberwar-for-now

conflict. I can understand why. Any geopolitical realists will assert that any available advantage in the chaotic international system is one to be taken. Maybe it is better that conflict does take place in cyberspace. Perhaps it's preferable to the carpet-bombing of cities or enslavement of nations, but for those of us who have watched cyberspace grow up in our lifetime, it is a disappointing development nonetheless.

"If you hide your ignorance, no one will hit you and you'll never learn."
Ray Bradbury, *Fahrenheit 451*

Let us hope that, with or without the aid of government, individuals will aggregate their efforts in the cause of keeping the two billion people connected in a global cyber commons rather than a patchwork of sovereign networks. To think that the system of states, which grew up from the last information revolution, the one surrounding the printing press, will operate unaffected by the most recent information revolution is short sighted. We likely live in a post-Westphalian time where governance is up to a multiplicity of actors, rather than the servants of sovereigns. That cyberspace's governance would be a construct of that time gives short shrift to human capacity for imagination and innovation.

That the Internet connects the computers used by a couple billion people represents a pointer to the sort of global community of the mind considered by Vernadsky or Teillhard de Chardin. This is the space in where discussion of Internet Freedom

comes to the fore. Is it a human right to live without censorship? A difficult question it is no doubt, but the Internet Freedom agenda also doubtlessly speaks more to value set of Western democracies that have embraced the concept. Asking to what degree the concept of completely unfettered access to Internet content (as long as that content doesn't violate copyright or other proprietary controls) is a universal right requires us to consider to what degree national and international political and economic interests and agendas can handle such freedom.

When we consider the issue of economic progress versus individual freedoms, China springs to mind. "For at least a century before 1949, major famines were probably frequent enough to warrant Walter Mallory's depiction of China in 1926 as the 'land of famine.'"[17] But since the 1958-1961 famine, China has been fairly successful in feeding its people, a relative afterthought in the fourth decade of rapid economic growth following Deng Xiaoping's reforms. Are the curbs on individual liberties a worthwhile sacrifice for stability, prosperity and full bellies? Lee Kuan Yew argued persuasively the plight of the under-developed global south and east.

> You're talking about Rwanda or Bangladesh, or Cambodia, or the Philippines. They've got democracy, according to Freedom House. But have you got a civilised life to lead? People want economic development first and foremost. The leaders may talk something else. You take a poll of any people. What is

[17] Cormac Ó Gráda, "Great Leap into Famine? – Ó Gráda's review of Dikötter book," *China Study Group*, March 15, 2011, http://chinastudygroup.net/2011/03/o-grada-review-of-dikotter/

> it they want? The right to write an editorial as you like? They want homes, medicine, jobs, schools.[18]

But the freedom of digital expression is but one of many concerns for the cyber politics of our planet. I use the term cyber not without consideration. There is a great over-use of the cyber appendage to all sorts of issues and debates. Saying "cyber" in Washington DC policy circles usually means cyber security, cyber warfare, the militarization of cyberspace – computers and war. At Freedom House or the National Democratic Institute, Internet Freedom is a desirable global good, much like the eradication of hunger, smallpox, or HIV. But it is also a rhetorical wedge. The American Internet Freedom campaign gathered steam in the weeks following Google's announcement regarding the company's information systems and theft of its intellectual property by actors in China. I employ cyberspace because it represents a technological infrastructure as well as an ideational area – it is a medium and a message. It makes business efficient, produces wealth unevenly, and perhaps most importantly, it allows individuals to connect to other individuals with a level of ease (but not necessarily a high level of reward) across great distance that did not exist before.

Because it has the capacity to permit social, economic and political reorganization, cyberspace is understandably feared. Think of all that Chinese hacking in the news

---

[18] Han Fook Kwang, Warren Fernandez, and Sumiko Tan, *Lee Kuan Yew, The Man and His Ideas*, Times Editions: Singapore, 1997.

or the massive piles of personal data accrued by the Silicon Valley social technology firms, led by Facebook and Google. (I omit Twitter and other micro-blogs from this discussion as there is no possible expectation of privacy in contributing 140 character bursts to the nascent noösphere.) There are all sorts of aggregators of data about which to be concerned – covert and overt, consensual and not – but to what end? I recently asked Christopher Soghoian whether he was more concerned by the infringements on privacy undertaken by government or private enterprise. To me, his response was one of seeing no difference.[19] This is interesting because it presents further evidence of our continued advance into a post-Westphalian period. The relative decline of state sovereignty has been a frequent topic of consideration since the end of the Cold War, but networked computers seem to have a degree of utility in political organization, and somewhat more ominously in campaigns designed to secure economic advantage or geopolitical positioning through covert action by cyber means.

Because of this cyberspace matters and is real enough as a venue of international politics from points across the soft to hard power spectrum. We must consider the change in how crisis and conflict are pursued and perceived today versus a generation ago. Then almost any conflict could be mapped to some segment of the East versus West overlay. The exceptions, such as the El Salvador-Honduras Football War, Turkey's invasion of Cyprus, and a few others, were aberrations. Rare was the conflict where Washington or Moscow had no skin in the game, but what

[19] Tech@State: Internet Freedom, March 8, 2013.

kept the game in check was the fear of escalation into the unfathomable terrain of nuclear Armageddon. In the last decade, the existential threat was the terrorist bomber. From an American perspective, that appears a problem well managed. It appears that the United States and its allies have the capacity to locate and monitor any jihadist who gets anywhere near pulling together the critical mass necessary to deliver a major blow against a significant population center. And when that individual has crossed the threat threshold, they are often swiftly dispatched by drone-launched precision guided weapon in one of the world's ungoverned areas – Pakistan's tribal areas, Yemen, the Horn of Africa, the list goes on.

Thus when we discuss national security related to the United States today, the topic boils down to two items: drones and cyber. John Horgan offers a powerful reminder of how political leaders in the United States should consider their country's strength in these two areas with a revisit of one of the world's older geopolitical primers, Thucydides' *History of the Peloponnesian War*. Although the United States has employed both these tools, although often veiled under the protection of covert action, it cannot expect them not to come back at it or its interests. That the United States can expect that no other power will employ a cyber weapon against it, its allies, or targets of strategic interest, the basis on its monopoly of use in cyber is likely to erode. Horgan suggests,

> [W]e should consider the fate of Athens, which at the beginning of the Peloponnesian War was Greece's major power. Athenian soldiers eventually

> overran Melos, killed all the men and enslaved the women and children. But just as the Melians had predicted, the cruelty and arrogance of Athens aroused opposition against it. Sparta and its allies eventually crushed Athens, which never regained its former glory.[20]

Cyberspace has come into being because it was allowed to grow by those who protected it, but never before has it appeared so challenged by forces of concern and outright fear. Paul Vixie recently argued, "We as a digital society are much better at strategies for coping than we are at strategies for remediation."[21] I would submit that international policymaking on cyberspace is of a similar character.

---

[20] John Horgan, "What Ancient Greeks Can Teach Us about Drones and Cyber-War," Scientific American, June 12, 2012, http://blogs.scientificamerican.com/cross-check/2012/06/12/what-ancient-greeks-can-teach-us-about-drones-and-cyber-war/

[21] Paul Vixie, "DNS Changer," *CircleID*, http://www.circleid.com/posts/20120327_dns_changer/