THE CONTEST OF THE CYBER COMMONS

Background Paper for 'Securing the Cyber Commons: A Global Dialogue'
March 27-28, 2011, The Munk School of Global Affairs, University of Toronto
By Rex Hughes, Visiting Fellow, Canada Center for Global Security

The new electronic interdependence recreates
the world in the image of a global village.
--Marshall McLuhan (1911-1980)
The Gutenberg Galaxy (1962)

For nearly half a millennium, international order has been constructed around a territorial-bound notion of state sovereignty as enshrined in the 1648 Treaty of Westphalia. State sovereignty has been the organizing principle for promoting both cooperation and conflict in the world system. But what happens when state sovereignty collides with the expanding digital continent of cyberspace in the early 21st century?[1]

On March 27-28, thought leaders from business, government, and the academy will gather at the new Canada Centre for Global Security Studies in the University of Toronto Munk School of Global Affairs to discuss the intersection of world order with cyberspace. Although, a mere science fiction term coined slightly over a quarter of a century ago by North American writer William Gibson, *cyberspace* is becoming a defining element of the 21st international affairs--especially, as it pertains to economic and military domains.

Although typically portrayed as a place where teenagers go to social network or play in virtual worlds, cyberspace has in recent years become a contested domain where states and other primary global actors increasingly compete for both comparative and strategic advantage. Leading countries are preparing to wage and win future wars in cyberspace, as demonstrated by the creation in the US of the world's first Cyberspace Command.[2] China and Russia are also at the forefront of developing offensive cyber capabilities in the form of the patriotic hacker and other covert government sponsored units, and several lesser powers have expressed their intent to develop offensive cyber capabilities.

Events of late, including the sophisticated Stuxnet attack directed against Iran's nuclear program and the government ordered Internet shutdown in both Cairo and Tripoli show the extent states are willing to go to defend their sovereignty in a non-territorial space. Some senior

[1] Misha Glenny, 'States embark on a scramble for cyberspace', *Financial Times*, March 17, 2010. http://www.ft.com/cms/s/0/05be0df8-3205-11df-a8d1-00144feabdc0.html
[2] Although the Canadian military lacks a formal Cyber Command, its land, sea, and air services already contribute important cyber defense capabilities to both NORAD and NATO.

military leaders have even argued that the first shot of the next major international conflict or war will be fired in cyberspace.

For liberal democracies with advanced information economies such as Canada, cyberspace can be seen both as a scary place as well as an opportunity space. Canadian ministries like those of other G20 democracies seek to keep citizens safe and secure in cyberspace as outlined in the recently published 'Canadian National Cyber Strategy' (2010). However, as Canada works towards a more secure cyberspace it must seek to do so while balancing core principles of liberty and justice that it closely cherishes. And due to the global interconnected nature of cyberspace, Canada cannot likely achieve these goals alone.

Even before the 17th century Treaty of Westphalia was drawn, European legal scholars and philosophers sought to create a universal body of principles and norms that would over time guide the creation of a shared global space or 'commons' where commerce and civic interaction could take place across national borders without hostilities. As the explorers and trading empires, including those of the Spanish, British, and Dutch, had begun to map the globe, such European thinkers as 17th century--Hugo Grotius, 18th century--Emer de Vattel, and 19th century--Fredrick Hegel recognized the potential for sustained international conflict in the commons in the absence of agreements to broad rules and regulations.[3]

The Law of the Seas (1994),the International Civil Aviation Treaty (1947), and the Space Treaty (1967) are all modern conventions that are rooted in this long tradition that seek to regulate the way the global commons are accessed and managed. Some legal and international relations scholars speculate that a 'Treaty for Cyberspace' or cyber arms control agreements are also needed to help regulate trade and military interactions in this unfolding domain.[4]

As a largely man-made domain, cyberspace differs vastly from the maritime realm, yet it shares some basic operating principles. US Adm. James Stravridis, NATO Supreme Allied Commander Europe (SACEUR), speaks and even blogs about the great 'Cyber Sea' where he compares cyberspace with the early ungoverned sea domain. In looking towards the future of global cyberspace governance Stravridis speculate that two major outcomes are possible: 1) International society unites to create a 'comprehensive set of rules and behavioral set of norms that would govern behavior within the cyber domain'; or 2) We enter a 'deterrence posture similar to the Cold War' where states and other primary actors are prevented from achieving maximum freedom of movement through the 'threat that harm will in turn' be done to them.[5] Although Stravridis prefers that international society pursue the former, he fears that the latter course may be more likely if cyberspace becomes more akin to an anarchical space. What then, will be the implications for liberty, justice, or free expression?

---

[3] For a more in-depth discussion of the political and philosophical roots of the global commons see Hersch Lauterpact's seminal 1933 work *The Function of Law in the International Community,* Clarendon Press, Oxford, 1933.

[4] Thus far the only significant treaty designed to regulate behavior in the cyber commons is the European Convention on Cybercrime (2004).

[5] 'Exploring the "Cyber Sea"' by Adm. Stravridis on the official website blog of the US European Command – *EUCOMversation*: http://useucom.wordpress.com/2010/02/

Outside of the Community of Democracies, there are several competing approaches to managing access to the cyber commons. These approaches are largely differentiated by unique ethnographic and cultural attitudes. As presently evident in the Middle East as well as in other democratically challenged regions, there are a number of national governments that seek to keep a tight control on the expansion and use of the Internet throughout their populations. Even successful authoritarian economies have sought to impose direct information censorship in order to regulate trade in information-based services. Consider the experiences of Google and RIM in countries where information freedoms are restricted on national security grounds.[6]

The new Canada Centre for Global Security Studies--the first Canada branded centre at the University of Toronto--has been created to educate and train a future generation of leaders that are well versed in the principles and norms of cyberspace governance. Additionally, they will learn specific technical skills that are crucial in the interconnected knowledge economy of the early 21st century. In order to enhance its geographical and cultural reach, the Munk School is developing partnerships with other leading universities around the world, including Cambridge, MIT, and Harvard. Other public, private, non-profit partnerships such as exists presently with SecDev, Palantir, and Google could develop as well. Representatives from these and many other distinguished organizations will meet in Toronto on March 27-28 to discuss the future of the Global Cyber Commons. During the two days of dialogue participants will discuss ideas and policies for developing a cyberspace that is both open and secure. Among the topics that will be discussed at this 2-day forum are those presented below and as taken from the recommended conference reading abstracts listed for the scheduled sessions.

Panel One: Liberation and Control: Contesting Cyberspace:

Every day there seems to be a new example of the ways in which human ingenuity combines with technology to further social change. For the Green Movement in Iran, it was Twitter; for the Saffron Revolution in Burma, it was YouTube; for the "color revolutions" of the former Soviet Union, it was mobile phones. No matter how restrictive the regulations or how severe the repercussions, communities around the world have exhibited enormous creativity in sidestepping constraints on technology in order to exercise their freedoms.

Looking at the seemingly endless examples of social innovation, one might easily assume that Internet-technologies possess a special power, that they are "technologies of liberation." No other mode of communication in human history has facilitated the democratization of communication to the same degree. No other technology in history has grown with such speed and spread so far geographically in such a short period of time. Twitter, to take just the latest web-application as an example, has grown from an average of 500,000 tweets a quarter in 2007 to more than four-billion tweets in the first quarter alone of 2010. The continual innovations in electronic communications have had unprecedented and far-reaching effects.

Yet some observers have noted that the very same technologies which give voice to democratic activists living under authoritarian rule can also be harnessed by their oppressors. Internet

[6] For an up-to-date map of global Internet censorship see the Open Net Initiative at http://map.opennet.net/

communications have made possible some very extensive and efficient forms of social control. Even in democratic countries, surveillance systems penetrate every aspect of life, as people implicitly (and perhaps unwittingly) consent to the greatest invasion of personal privacy in history. Digital information can be easily tracked and traced, and then tied to specific individuals who themselves can be mapped in space and time with a degree of sophistication that would make the greatest tyrants of days past envious. So, are these technologies of freedom or are these technologies of control?

Larry Diamond in "Liberation Technology" argues that the Internet, mobile phones, and other forms of "liberation technology" enable citizens to express opinions, mobilize protests, and expand the horizons of freedom, but he cautions that autocratic governments are also learning to master and deploy these technologies. For activists this means that their ability to harness the democratizing effects of technology may be limited by regimes that seek to equally exploit its surveillance and monitoring capabilities. For Diamond and other techno pragmatists, the outcome of the contest between democrats and autocrats will depend not just on technology, but on political organization and strategy.

Evgeny Morozov of the New America Foundation and Stanford paints an even bleaker picture for the future of Internet freedoms. In his recently published book Net Delusion. Morozov issues a stinging rebuke of what he calls 'cyber utopianism'. In his book and subsequent article, Morozov's argues that socially minded techno activists have put too much faith in the ability of the Internet and other social media to transform authoritarian states into liberal democracies. For Morozov so called 'liberation technologies' can equally be used by authoritarian regimes to crush democratic movements. Morozov accuses Western democratic officials of operating with a "voluntary intellectual handicap' by assuming that Internet technologies are always democratic. To combat this handicap Morozov calls for 'cyber realism' to replace 'cyber utopianism'. To this effect Morozov believes that Western officials and activists should be more cognizant of the limits of Internet technologies when attempting to liberate oppressed peoples.

What role do social network technologies play in the revolutions of the Middle East and North Africa? Did Facebook and Twitter actually play a consequential role in regime disruption? How can the Internet be used as tool of control? In what ways is cyberspace being contested today? What role, if any, should liberal democratic governments have in protecting cyberspace as a global commons? Should governments, media, activists, and corporations be active supporters of Internet freedom? What are the risks?

Panel Two: Commerce and Control: Economics of the Cyber Commons

Since the commercialization of the Internet in 1994, cyberspace has been associated with free and open commerce governed by few constraints or regulations. However, it more recent years, the laissez faire spirit of the Internet has come under increasing attack by governments seeking to impose new rules and regulations. Among American high-tech firms, Google has been especially vocal about the increasing proclivity of the state to employ censorship as a trade barrier.

In the Google white paper 'Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information', Google advocates argue that the transformative economic benefits of the Internet are under threat, as increasing numbers of governments move to regulate information flow. In order to remedy the increased proclivity of governments to use censorship as trade barrier, Google contends that the international community must take action to ensure the free flow of information online. In the Google view governments should honor existing international obligations including the World Trade Organization (WTO) agreement, prevent trade barriers created by information regulation, and develop new international rules that provide enhanced protection against these trade barriers of the 21st century.

Google further argues that in order to realize the full potential of the Internet as a global marketplace and platform for innovation, policymakers in the United States, the European Union, and elsewhere should pursue three steps to break down barriers to free trade and Internet commerce: 1) Focus on and publicly highlight as unfair trade barriers those practices by governments that restrict or disrupt the flow of online information services; 2)Take appropriate action where government restrictions on the free flow of online information violate international trade rules; and 3) Establish new international trade rules under bilateral, regional, and multilateral agreements that provide further assurances in favor of the free flow of information on the Internet.

Privacy and Freedom of Expression

In recent years several leading Western high-tech firms have been accused of violating basic human rights principles by aiding autocratic regimes in their question to crush dissenting voices. Yahoo, Microsoft, Google, RIM, are among these companies. Executives from the accused companies have been called to testify before parliamentary bodies in the US, Canada, and the EU re: their potential role in aiding non-democratic regimes that have sought personal or private information about their customers. Telecommunications firms have also stood accused of installing surveillance technologies at the request of governments that seek to spy on their citizenry.[7] More recently several European mobile vendors stand accused of providing text logs to Egyptian authorities during the recent uprising against the Mubarak Government.

In 2008 The Global Network Initiative (GNI), was established by a consortium of public and private stakeholders as a means of advancing human rights in cyberspace with a focus on promoting best practices of American high-tech firms overseas. Since its establishment, the GNI has sought to champion numerous initiatives concerning both the protection of privacy and freedom expression online.

In his paper "Protecting Privacy and Expression Online: Can the Global Network Initiative Embrace the Character of the Net?", Colin M. Maclay discusses how a multistakeholder NGO, the Global Network Initiative (GNI), has emerged as a forum for industry and activists to work together to establish a code of conduct when selling wares within non-democratic markets. Participants in the GNI include nongovernmental organizations, ICT companies, investors, and academics. Maclay describes GNI's collaborative structure and intentions, explores several

[7] In 2007, the House Foreign Affairs committee accused Yahoo! of providing false testimony in a human rights case that sent a Chinese journalist to prison for a decade.

concerns, and highlights some of the challenges GNI must address to fulfill its intended purpose. Issues that will impact success include the tensions among structure and flexibility, aspiration and practicality, and refining known approaches and creating new ones. As both an independent research and GNI board member, Maclay believes that the GNI 'clearly lacks culturally and geographically diverse participation, and is likewise limited in terms of the range of participating organizations within sectors, and companies in particular. . . .' He also admits that from GNI and related efforts 'causes of success and failure will not always be clear' and is open to 'new kinds of institutions and new approaches to policymaking'. Perhaps cyber arms control or conventions?

In "Shi Tao, Yahoo!, and the Lessons for Corporate Social Responsibility," Rebecca MacKinnon, chronicles the case of Chinese journalist Shi Tao was convicted and sentenced to ten years in prison for leaking state secrets abroad. Key evidence cited in Chinese court documents included information about Shi's account supplied by Yahoo! to the Chinese State Security Bureau. Condemnation by human rights groups and investors, U.S. congressional hearings, a Hong Kong government investigation, and a U.S. lawsuit followed. McKinnon in her paper documents the core facts, events, issues and debates involved.

The Shi Tao case highlights the complex challenges of corporate social responsibility for Internet and telecommunications companies: They are caught between demands of governments on one hand and rights of users on the other – not only in authoritarian countries such as China but in virtually all countries around the world. While there are no simple or quick solutions, Internet and telecoms companies seeking to establish trustworthy reputations across a global customer base cannot afford to ignore the human rights implications of their business practices. Users and investors have a right to demand that user rights be respected. If companies fail to respect user rights, the need to develop non-commercial, grassroots alternatives will become increasingly important if privacy and free expression are to be possible anywhere.

Thus, should Internet censorship be considered a barrier to trade? What responsibilities do private sector actors have to preserve cyberspace as an open commons? Are self-governance mechanisms, like the Global Network Initiative, enough or do private sector actors need to be regulated to respect human rights?

Panel Three: Crime and Control: Balancing Privacy and Law Enforcement

In early Internet days, cyberspace was largely free of major crime. However, the Internet's transformation from a research network into a major global platform for commerce and banking has made it a top target for organized crime. Response to the Internet's growing criminal element, around the world law enforcement is scrambling to beef up capacity and capabilities fight serious online crime. From financial fraud to child pornography, law enforcement seeks to prevent the Internet from becoming an anarchical space. The Citizen Lab is among leading research institutes that have pioneered the study of criminal activity in cyberspace. Most

recently its Koobface study led by Ron Deibert and Rafal Rohozinski has shown how criminal networks have exploited social networking technologies for economic gain.

According to Deibert and Rohozinski, cybercrime thrives not just because of ingenuity and lawlessness, but because of social media opportunities. The Koobface worm (an anagram of Facebook) succeeds by mimicking normal social networking behavior. According to Deibert and Rohozinski, Koobface is like a digital amoeba, living parasitically on people's sharing habits. It leverages the most successful of all age-old criminal techniques with new habits – our readiness to extend trust – with our eagerness to click on links. Through the proliferation of social networking technology people have become conditioned into a world of intense social interaction. And it is that conditioned tendency that Koobface exploits with precision. In order to combat this growing menace, Deibert and Rohozinski call for greater engagement by law enforcement bodies.

Educating Lawmakers

In recognizing the need for its member states to develop more national capacity to fight cybercrime, the ITU has developed a "Toolkit for Cybercrime Legislation" The Toolkit aims to provide countries with sample legislative language and reference materials that can assist in the establishment of harmonized cybercrime laws and procedural rules. The Sample Language provided in the Toolkit, while not a model law, was developed after a comprehensive analysis of the laws of developed nations and the Council of Europe (CoE) Convention on Cybercrime. The Toolkit language is consistent with these laws and is intended to serve as a guide for countries desiring to develop, draft, or modify their own cybercrime laws. The Toolkit is intended to advance the global harmonization of cybercrime laws by serving as a central resource to help legislators, attorneys, government officials, policy experts, and industry representatives around the globe move their countries toward a consistent legal framework that protects against the misuse of ICTs.

In Canada businesses and law enforcement agencies are increasingly interested in learning who is doing what online. In "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," Daphne Gilbert, Ian R. Kerr, and Jena McGill argue that Canadian law enforcement is making steady progress in developing tools and techniques to fight cybercrime. In their study the authors investigate the changing role of TSPs from gatekeepers of privacy to active partners in the fight against cybercrime. The authors also argue that the legislative approach provoked by the Council of Europe's Convention on Cybercrime (that is soon to be adopted in Canada) will lower the threshold of privacy protection and significantly alter the relationship between TSPs and individuals. Persistent client state http-cookies, keystroke monitoring and a number of other surveillance technologies have been developed to gather data and otherwise track the movement of potential online customers. Many countries have enacted legislation that would require telecommunications service providers (TSPs) to build a communications infrastructure which would allow law enforcement agencies to gain access to the entirety of every telecommunication transmitted over their facilities. Canada is considering doing the same.

Criminologists have also joined the call for more innovative law enforcement techniques to curtail growing cyber criminality. David Wall has argued in "Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace" that the Internet and the criminal behavior it transforms (cybercrime) pose considerable challenges for civic order maintenance and law enforcement because Internet-related offenses take place within a global context while crime tends to be nationally defined. Policing cyber-crime is made all the more complex by the very nature of policing and security being networked and nodal and also because within this framework the public or community police play only a small part in the policing of the Internet. In this paper it is argued that the future role of the public police in monitoring Internet-related transgressions is more than simply acquiring new knowledge and capacity, for it is about forging new relationships with the other nodes within the networks of Internet security. According to Wall these relationships require a range of transformations to take place in order to enhance the effectiveness and legitimacy of the nodal architecture. It will then be argued that some of the contradictions faced by 'the police' are being reconciled by the gradual reconstitution of a neo-Peelian paradigm across a global span, which brings with it a range of instrumental and normative challenges.

Do we need to give law enforcement and intelligence more powers to police cyberspace? Do states have too much, or not enough, surveillance powers in cyberspace? Who is watching the watchers?

Panel Four: War and Control: Deterrence and Arms Control in Cyberspace

Cyberspace is considered the 5th battlespace as proclaimed months ago by officials in the US Dept of Defense. But if cyberspace is also an anarchical space, then what if anything can be done to regulate or deter warfare in the virtual domain? James Farwell and Rafal Rohozinski in "Stuxnet and the Future of Cyber War," chronicle the Stuxnet attack on an Iranian nuclear facility at Natanz. According to Farwell and Rohozinski, the sophisticated nature of the Stuxnet attack suggests that for cyber war, the future is now. Yet according to these authors what is more important is the political and strategic context in which new cyber threats are emerging, and the effects the worm has generated in this respect. The authors also draw attention to the confluence between cyber crime and state action. States are capitalizing on technology whose development is driven by cyber crime, and perhaps outsourcing cyber attacks to non-attributable third parties, including criminal organizations. Together these authors see great potential for striking at enemies with less risk than using traditional military means. However, while it is unclear how much the Stuxnet program cost, it was almost certainly less than the cost of single fighter-bomber. Yet if damage from cyber attacks can be quickly repaired, careful strategic thought is required in comparing the cost and benefits of cyber versus traditional military attack.

In "Cyberwar as a Confidence Game," Martin Libicki askes if cyberwar the twenty-first-century version of nuclear war? Libicki notes that readers of the Economist, whose 3–9 July 2010 cover portrayed a digitized nuclear explosion in the midst of a city, could be forgiven for such thinking.

For Libicki the takeaway was obvious: cyber weapons are now the latest class of strategic weapons; they can do enormous damage to societies; and the first recourse against this threat should be some sort of arms control. Otherwise, the bad old days of strategic confrontation would be back, but this time with scores of countries and no small number of non-state actors, with transnational criminal organizations, and with a few overindulged high school students having the requisite capability to build weaponry that can bring life as we know it to a prompt halt. Such a scenario could happen, but Libicki sees danger in seeing cyber weapons as primarily strategic in the same way as nuclear weapons.

Thus, Libicki argues that a more plausible strategic rationale for the United States' developing cyber weapons is to make other states think twice about going down the road toward network-centric warfare as the United States is doing. Sophisticated cyber weapons likely have the capability of making other states—already lacking confidence in their ability to handle high technology—doubt that their systems will work correctly when deployed, particularly if used against the United States or its nation friends.

However, some cyber defense experts believe the US could be losing the cyber war. According to Mike McConnell the United States is fighting a 'cyber-war' today, and according to him it is a war that it is losing. As the most wired nation on Earth, McConnell worries that the US offers the most targets of significance, yet its own homeland cyber-defenses are woefully lacking. The stakes are enormous. To the extent that the sprawling U.S. economy inhabits a common physical space, it is in its communications networks. According to McConnell, if an enemy disrupted financial and accounting transactions, US equities and bond markets or retail commerce, chaos would result. McConnell speculates that power grids, air and ground transportation, telecommunications, and water-filtration systems would also be in jeopardy. These battles are not hypothetical. Google's networks were hacked in an attack that began in December and that the company said emanated from China. And recently the security firm NetWitness reported that more than 2,500 companies worldwide were compromised in a sophisticated attack launched in 2008 and aimed at proprietary corporate data. Indeed, the recent Cyber Shock Wave simulation revealed what those involved in national security policy have long feared: US war games and strategy documentation focused on traditional warfare while failing to address the most basic questions about cyber-conflicts.

One year following the establishment of the US Cyber Command or USCYBERCOM, Michael V. Hayden (former US National Security Agency director and retired US Air Force General) in a paper "The Future of Things 'Cyber'" stated that current US policy, law, or doctrine is adequate to achieve US strategic objectives in cyberspace. Most disappointingly according to Hayden — the doctrinal, policy, and legal dilemmas that currently face the US remain unresolved even though they have been around for the better part of a decade. Thus, Hayden thinks now is the time to think strategically about US strategic objectives in cyberspace.

But if cyberspace really has become an anarchical space and a fifth Battlespace, then what can be done to regulate it? In a May 2009 New York Times commentary, Ron Deibert sees the creation of the US Cyber Command as taking a step towards escalating conflict in cyberspace.

Thus, Deibert expresses what a growing chorus of experts sees as the need for the creation of a global cyber arms control regime. In his 2010 article "A Treaty for Cyberspace," Rex Hughes argues that it is time to consider the formation of such a regime. As cyberspace evolves from a technology enthusiast's domain into a global economic and military 'battlespace', Hughes argues that there is increased likelihood of a major interstate cyber conflict in cyberspace. Thus, Hughes advances that international society needs to begin working towards the drafting and ratification of a global cyber treaty. While Hughes does acknowledge that a cyber arms control regime is a distant possibility, he does join those who argue that some restraints should be put on future cyber attacks or warfare. For Hughes, the questions then arise as to which countries are best to lead the creation of such a regime and through which fora should such a regime develop. He supports the Deibert concern that the military approach without a cyberspace convention or treaty likely threatens the concept of the open Internet the means to prevent an actual conflict or war in cyberspace.

Should the United States demonstrate its offensive cyber capabilities as an exercise in deterrence in cyberspace? Under what conditions is a computer network attack an 'act of war'? Are states responsible for computer network attacks and espionage that originate in their territory, even if they are not directing those acts? Does the concept of cyber arms control or a cyberspace treaty have any merit?

#######