Georgia Tech | School of Public Policy

Workshop on Political Space and Cyber Space

May 19 and 20, 2016
Yellow Jacket Conference Room,
GTRI, 6th Floor, Centergy Building,
75 5th St. NW (Tech Square),
Atlanta, Georgia 30318

Workshop description

This workshop/joint research project explores the tensions and intersections between political territory and cyberspace, focusing on their implications for governance institutions and for security policy. It will bring together experts in international relations, political geography, political science, network measurement, cybersecurity, Internet governance, trade and Internet of things.

igp
Internet Governance Project

Territory is a core concept of political authority, as sovereigns hold supreme authority in their domestic territory and exclude other sovereigns at their borders. Digital networks have created a tension between territorial space and the globalized virtual territory called cyberspace. Communication via the Internet creates new virtual spaces that are not aligned with political geography.

While it is possible to see and document technical adaptations of cyberspace to territorial domains, and vice-versa, in our view the policy and governance problems posed by their intersection remain largely unsettled. How can states, multinational businesses, communities, and individuals negotiate the misalignment between the Internet's geographically unbounded information flows and the political and legal systems' emphasis on well-defined, stable jurisdictional borders? The resolution of these problems has profound practical implications for all aspects of global order, but also poses interesting puzzles in computer science, international relations, public policy and institutional theory.

Schedule

Thursday, May 19

13:00 – Welcome and Introductions

13:30 - 15:00 – **The conceptual and theoretical** (Hans Klein, moderator)

- How valid and useful are current conceptualizations of the relationship between cyberspace and political space? What alternative conceptualizations exist?

Speakers: Corey Johnson, Sandra Braman, Milton Mueller, Jennifer Daskal

15:00 - 16:30 – **Governance regimes** (Corey Johnson, moderator)

- What kind of useful parallels exist between institutionalized recognition of territory in cyberspace and in other domains, such as the oceans, the Arctic and outer space?

- How do the tensions between territory and cyberspace affect the nature of political identity, and the expectations and practices associated with citizenship?

Speakers: Marial Borowitz, Patricia Vargas-Leon, Farzaneh Badii

16:30 - 19:00 – Drinks: Community Smith Garden 2nd F, Renaissance Hotel, 866 West Peachtree St NW, Atlanta, 30308 (walking distance from the venue)

19:00 – Dinner: Community Smith Restaurant,
The Greenhouse 1st F, Renaissance Hotel, 866 West Peachtree St NW, Atlanta, 30308

Friday, May 20

9:00 - 10:30 – **The technical/operational** (Wenke Lee, moderator)

- How effective are current techniques of bounding information to a specific territory and what counter-measures are being used to get around them?

- Which new developments in computer science, blockchain and network engineering are salient?

Speakers: Mark Gondree, Ron Deibert, Eli Dourado

(Break)

11:00 - 12:30 – Governance Between and Among Territories: The Military and Strategic (Moderator, Seymour Goodman)

- How is the concept of defending or attacking “our” territory in cyberspace differentially articulated and operationalized in the military and security contexts at different levels of network architecture?

- BRICS and great power rivalries over Internet governance

Speakers: Sandra Braman, Hans Klein, Jyoti Panday, Tatiana Tropina

12:30 - 13:30 – Lunch

13:30 - 15:00 – **Governance Looking Out: Trade, Finance, and Territorialization** (moderator: Milton Mueller)

- Data localization, 'data sovereignty' and the cloud

- Geoblocking and copyright

- Bitcoin and capital controls

Speakers: Susan Aaronson, Louis Pauly, Peter Swire, Eli Dourado

(Break)

15:30 - 17:00 – Overview and discussion.

Jennifer Daskal, Louis Pauly, rapporteurs

18:30 - 19:00 – Drinks Ponce City Market, 675 Ponce De Leon NE, Atlanta

Meet inside at Bellina Alimentari Bar (Ponce City Market is not walking distance from the hotel or workshop venue; we will organize taxis and cars from the Indigo)

19:00 – Dinner (sponsored by Texas A&M University) Two Urban Licks restaurant 820 Ralph McGill Blvd NE, Atlanta, 30306 (15 minute walk from Ponce City Market along Beltline)

Participants (alphabetical)

Susan Aaronson	Research Professor, Elliot School of International Affairs, George Washington University
Farzaneh Badiei	PhD student, Hamburg University
Sandra Braman	Abbott Professor of Liberal Arts & Professor of Communication, Texas A&M
Jennifer Daskal	Assistant Professor, American University Washington College of Law
Ron Deibert	Professor, University of Toronto and Director, CitizenLab
Eli Dourado	Research Fellow, Mercatus Center, George Mason University
Seymour Goodman	Professor, School of International Relations, Georgia Institute of Technology
Mark Gondree	Security researcher, Computer Science Department, Naval Postgraduate School
Corey Johnson	Associate Professor, Department of Geography, University of North Carolina Greensboro
Wenke Lee	Professor and John P. Imlay Jr. Chair in the School of Computer Science, Georgia Institute of Technology
Hans Klein	Associate Professor, Georgia Institute of Technology
Milton Mueller	Professor, Georgia Institute of Technology
Jyoti Panday	Researcher, Indian Institute of Management, Ahmedabad Idea Telecom Centre of Excellence
Louis Pauly	Professor, University of Toronto
Peter Swire	Huang Professor Georgia Institute of Technology Scheller School
Tatiana Tropina	Senior Researcher, Max Planck Institute for Foreign and International Criminal Law
Patricia Vargas-Leon	Ph.D. student, Syracuse University

Abstracts

The conceptual and theoretical

Alignment and 'Fragmentation': When Cyberspace meets Sovereignty

Milton Mueller, Professor, Georgia Institute of Technology, School of Public Policy

One of the clearest and most consequential confrontations between political space and cyberspace is the contemporary policy debate over the so-called "fragmentation" of the Internet caused by efforts to assert 'data sovereignty' or other forms of control over Internet services. This paper examines that controversy and links it to theories of sovereignty. It mounts a critique of both the advocates of "data sovereignty" and of the "fragmentation" meme. The argument is based on 6 theses:
1. Current attempts to define what "fragmentation" means in cyberspace leave much to be desired. It usually conflates technical fragmentation/incompatibilities with completely different phenomena such as data localization or content filtering; 2. That conflation is dangerous because the internet is by its very nature 'unifragged;' i.e., it is a network of networks that relies on globally compatible protocols and identifiers but empowers each network operator at the AS level to selectively manage their exposure to the global internet; 3.Technical fragmentation is not happening; the policy and internet governance debates over fragmentation are really about alignment; which the paper defines as the subjugation of the cyber domain to the territorial jurisdiction of the state; 4. States are asserting sovereignty via alignment, but perfect alignment is not attainable without destroying the internet; 5. In Political Space, the linkage between sovereignty and territoriality is often asserted but under-theorized and poorly explored; 6. It is possible to conceive of cyberspace as a sovereign space governed by a non-national polity.

Governance regimes

Analyzing Governments' Regulatory Practices over Global Resources: Comparing the Law of the Sea and Cyberspace

Patricia A. Vargas-Leon, PhD Candidate, School of Information Studies, Syracuse University

The purpose of this paper is to analyze the implications of a potential cyber-space regime based on the ocean division criteria established by the United Nations Convention on the Law of the Sea (UNCLOS). The paper will attempt to determine the state practices and arguments nation-states (represented by their governments) followed to regulate global resources beyond their own jurisdictions.
The paper performs a case-study of the third conference on the law of the sea (1973-1982), the outcome of which was UNCLOS. Following a historical legal perspective, this paper will: a) provide an overview of state practices and arguments to delimit the oceans since ancient times until the second conference on the law of the sea from 1958, b) analyze the negotiations and arguments that governments used to try to delimit the seas of the world during the third conference on the law of the sea from 1982, and c) compare the elements identified from the analysis of the third conference on the law of the sea to today's cyber-security policy debate. The paper focuses on two types of arguments used in efforts to define boundaries in the ocean: national defense and economics. Throughout world history, the ocean division criteria have been derived from the coexistence of these two arguments or from the preeminence of one over the other. Today, similar arguments provide the legal and political basis for global cyber-security policies. In that way, this paper will be an attempt to understand the implications that the delimitation of the oceans might have for the governance of cyber-space, and to learn from past experiences where governments conducted negotiations to try to take control over spaces beyond their own territories.

Abstracts

Infrastructure, Attribution, and Deterrence in Space and Cyberspace

Mariel Borowitz, Assistant Professor, Georgia Institute of Technology, School of International Relations

In the past fifty years, space and cyberspace have become integral infrastructural elements that underpin global commercial, civil, and military applications. While not always visible to the end user, smooth operation of this infrastructure is essential for maintaining both routine daily activities as well as major military actions. Attacks on this infrastructure are tempting for adversaries interested in causing economic harm or reducing the ability of the United States to project military force. However, unintentional errors can occur in both realms, and correctly attributing the source of malfunctions can be challenging. In this environment, deterring aggressive or irresponsible actions is difficult. This presentation will provide an overview of existing agreements that govern activities in space, including the Outer Space Treaties, and discuss ongoing efforts to define new agreements to develop "rules of the road" for operating in outer space and to deal with intentional and unintentional creation of space debris. The presentation will examine the applicability of these efforts to cybersecurity challenges.

Do states have sovereignty over ICANN's delegation of ccTLDs?

Farzaneh Badii, PhD candidate, Hamburg University Law and Economics program

Governments are keen on asserting sovereignty rights over ccTLDs. They claim that sovereigns should bethe ultimate authority over delegation and public policy for ccTLDs. In countries like Iran with a long-term conflict with the US, sovereignty rights are thought to immunize them from confiscation by outsiders. Some sovereignty claims closely mirror property claims. In physical space, sovereign states have recognized territories. Sovereignty results primarily from a state's ability to maintain a monopoly on the legitimate use of violence in that territory, but also from recognition of its sovereignty by other states. In cyberspace, the delegation of a domain name representing a country (e.g., .BR for Brazil, or .IN for India) involves an unusual three-party relationship between a government, a party that operates the domain (delegee) and ICANN. ICANN, as the global coordinator and policy maker for the domain name space, must delegate a country code or name to a specific operator – otherwise the domain simply does not exist on the Internet. And because the DNS root is a globally shared resource, its management involves more than the wishes of the sovereign state but also involves obligations to "the global Internet community. " Yet, as a nonprofit under U.S. federal and California jurisdiction, ICANN's role seemingly subjects ccTLD delegees to civil law claims of the sort seen in the Iran and Congo cases. This research looks into the practical implications of the obligations of states to global Internet community over ccTLD delegations and whether asserting domestic sovereignty over the delegation of ccTLD is effective in ICANN governance.

The technical and operational

Extraterritoriality and Mutual Entanglement in Cyberspace
Ron Deibert with Louis Pauly

As the Internet developed and spread in popularity in the 1990s and early 2000s, many predicted it would present a major challenge to state sovereignty and authoritarian rule. Some went so far as to forecast a coming borderless world, or even the dissolution of organized government altogether. More recent research has emphasized the opposite: growing state controls over cyberspace within territorial boundaries. My own research via the Citizen Lab and its associated projects (like the OpenNet Initiative) has been one of the main contributors to this correction. Over the last decade, using a mixed methods approach that has combined area studies, field research, legal and policy analysis and network measurement techniques, we have documented several generations of state-led information controls. These findings have been echoed by the research of a growing number of other scholars, and noted with concern by activists, businesspeople, and policymakers. While the trends towards territorialization in cyberspace are undeniable, the growing recognition of and concern about these trends may have obscured the extent of which states simultaneously project power in and through global cyberspace outside of their territorial jurisdictions. In other words, growing state power in cyberspace does not stop at the border; there are extraterritorial projections of state power through cyberspace that are becoming more elaborate and far reaching. Not surprisingly, the most extensive of these projections come from the United States, but even the most autocratic regimes most associated with "cyber Westphalia" project power extraterritorially in cyberspace. States project power extraterritorially through cyberspace to better acquire data about the world around them: to anticipate, analyze, and interdict threats; to shape the political environment to their strategic advantage; to support other forms of material power that are also constituted globally, like the movement of goods and services, transportation, and armed forces, and to engage in the broad command and control of their interests. The combined unintended "network effect" of all states engaging in extraterritorial projections of power through cyberspace is to support the continuation and expansion of globalization processes, and the mitigation of state competition, particularly with respect to disruptions to cyberspace itself (upon which states, and state elites, depend). Drawing from recent Citizen Lab research into state espionage and targeted digital attacks, we describe several examples of extraterritorial projections of state power. We conclude with some commentary ton what these practices mean for security, power, and authority in global politics.

New Trends in Oppositional Geolocation
Mark Gondree, Computer Science, Naval Postgraduate School

In 2009, Muir and Van Oorschot surveyed technologies for Internet geolocation and considered their behavior in adversarial settings. They find many technologies proposed for policy enforcement based on IP geolocation---such as digital content restrictions and credit card fraud monitoring---were deficient and, ultimately, susceptible to adversarial manipulation. We update this early work, discussing IP geolocation, user geolocation, IP address extraction, data geolocation and data center geolocation in adversarial settings. We find many proposed techniques are susceptible to adversarial manipulation in the same ways considered by Muir and Van Oorshot; however, more recent results have demonstrated attacks against those schemes originally considered less susceptible. We also highlight and resolve an apparent contradiction between two separate, recent claims (that delay-based data geolocation can be manipulated arbitrarily by a powerful adversary adding delays, and that it is not meaningfully susceptible to delay-adding attacks) arguing the method for summarizing the statistical results is likely the root cause of these polar-opposite claims. We also propose possible avenues for new research.

Governance Between and Among Territories: The Military and Strategic

Russia and Internet sovereignty: Internal and External Myths of the "Cheburashka network"

Tatiana Tropina, Sr Researcher, Max Planck Institute for Foreign and International Criminal Law

Are there any connections between Internet governance and a beloved Soviet cartoon character Cheburashka, a small furry beast with very large ears and big cute eyes? Probably no one could imagine such a link until April 2014, when Russian media reported that a Russian senator, Maksim Kavdzharadze, had proposed to create a 'Russian Internet,' separate from the US and Europe, and name it "Cheburashka." The senator dismissed his statements a day later, stating that he doesn't support any digital Iron Curtain; however, this incident reflects more serious processes and issues in Russian Internet governance policy. Since the beginning of the 2000s, Russia is well known for its efforts to challenge the multi-stakeholder concept of Internet governance by raising sovereignty and security concerns and by demanding a greater role for national governments in what is considered to be control over the Internet. However, the narratives and efforts that Russian policy makers use to promote Internet sovereignty are not always coordinated, and frequently reveal a lack understanding of fundamental issues. There are a number of misconceptions both in domestic and foreign policy that make the Russian approach to Internet sovereignty incoherent and alienate Russia from the rest of the world even when it's trying to come up with otherwise reasonable policy initiatives. The goal of the presentation at the workshop (and, later, a paper focusing on these issues) is to debate the narratives and concepts most frequently associated with Russian attempts to "control" the Internet.
The author initially divides the issues into the following categories: 1) misunderstandings related to cyber-threats; 2) Russia's agenda on norm-making processes at intergovernmental fora; 3) the narratives of the decision-making elites, and 4) Russian domestic policy and legislative initiatives related to "control" over the Internet. Finally, the author will conclude by identifying the broader problem: the lack of understanding in Russia of what the multi-stakeholder governance model and hands-off regulation mean. The presenter will argue that the confusions related to multi-stakeholder model stem from the process of telecommunication liberalization, or rather the lack thereof, in the Russian market and the absence of experience in dealing with any form of governance than state control.

Synchronizing Sovereignty: India's uneven aims and fragmented strategies in cyberspace

Jyoti Panday Program Officer, Center for Internet and Society, India

This paper examines India's policy initiatives and decision making through its engagement with internet governance instruments and processes, territorialization of data and the militarization of cyberspace. Understanding India's stance in cyberspace is not easy given the shifting policy positions articulated by dominant institutions and actors over the years. The common perception amongst most observers has been that India's response to cyber related issues has been marked by a slow learning curve which has resulted in engagement that is more reactive than guided by a long-term vision.
While I do not contest this interpretation, such a characterization does not lend itself to the unique and complex challenges India faces in cyberspace, nor does it allow for the development of a broader framework for the study of its Internet related policies. In developing a scheme for India's stance in cyberspace evaluating its current policy choices from the perspective of exertion of the principle of sovereign supremacy may serve as a helpful starting point. There are a number of examples of India's attempts to exert the notion of sovereignty and territoriality in the context of cyberspace both at the international and national levels. This paper aims to address some of these limitations evaluating India's decision-making across three most critical internet related issues: internet governance, its attempts at territorialization of data and efforts at the militarization of cyberspace. The issues included in this study are not meant to document the full spectrum of the State's interaction with the notion of sovereignty in cyberspace. Rather, the issues provide three interesting examples that are of relevance to the current environment. Other issues that are important but beyond the scope of this paper include issues of copyright, cyber crime, and the rising cost of the Internet and access. (continued)

Synchronizing Sovereignty: India’s uneven aims and fragmented strategies in cyberspace
(continued)

By focusing on the issues highlighted above, I aim to demonstrate that India’s approach to cyberspace draws from its experiences both historical and those triggered by certain new developments within India and abroad. While a study of the responses to these issues is unlikely to show an overarching theme, they provide context to how the notion of sovereignty has become a pivot point that guides India’s stance in cyberspace. In this I will also show India’s preference for a central role of the state in internet related issues has been a persistent theme has been internalized by the Indian leadership and bureaucracy and cuts across issues and sectors. In exploring India’s position from these three frameworks my objective is to show that its multi-pronged strategies striving for a larger role of the State is not working in a stable fashion. Rather India’s current approach creates contradictions and tensions that are undermining traditional forms of sovereignty. Further, my analysis reveals that three common guiding principles have emerged in India’s policy stance across the frameworks for its interactions being evaluated in this paper.

Foreign Propaganda or Domestic Empowerment? Assessing the Content of Russia’s RT.com

Hans Klein and Rebecca Harris, Georgia Tech

Sovereignty is of two types: internal and external. Internal sovereignty concerns state-society relations and is based on the norm that the state possesses supreme domestic authority. External sovereignty concerns inter-state relations and is based on the norm of mutual autonomy and non-interference in domestic affairs. Both types of sovereignty are spatially defined: the border of a country’s territory demarcates the internal-external boundary.Each type of sovereignty faces challengers. Internally, the state is challenged by society: social groups may critique the legitimacy of state institutions and practices and may actively challenge state power. Externally, the state is challenged by other states, who may also critique state institutions and actively challenge state power. Although they may pursue different ends – better domestic governance (internally) vs. regime change (externally) – the two challengers share a common interest in critique and change. Cyberspace has made it increasingly possible for these two groups to act on their common interest. In particular, cyberspace allows external states to communicate in domestic media spaces, thereby promoting domestic social challenges to state supremacy. In this paper we analyze this phenomenon in the context of US society. US audiences now have access to Russia’s cyberspace-based news source, RT.com, whose programming gives voice to domestic critics of the US government. Prior to the advent of RT.com, US social criticism was largely located on non-profit FM radio, public access TV, and other “alternative media” that were (and still are) fragmented, poorly funded, and relatively ineffective. RT.com, however, benefits from hundreds of millions of dollars of Russian funding, which allows it to provide a resource-richer and more professional platform for criticism of the US government. The effectiveness of RT.com can be inferred by its portrayal in the US mainstream media, where it has evolved from being the beneficiary of bemused praise to being the target of damning accusations. This paper analyzes RT.com to assess whether it is Russian propaganda (as alleged in recent Time magazine coverage and in Congressional hearings) or whether it is an instrument that empowers legitimate domestic critique (as it itself alleges.) In the paper we perform a content analysis of invited speakers on RT.com and assess whether they represent foreign/illegitimate viewpoints or whether they represent domestic expert/legitimate viewpoints. We conclude with speculation about the positive and negative aspects of external empowerment of domestic social groups.

Cybersecurity and Occupation: Vulnerabilities of the State in the Tallinn Manual

Sandra Braman, Abbott Professor of Liberal Arts, Texas A&M University

The detailed consideration of the ways in which existing international law pertains to cybersecurity in the Tallinn Manual includes not only a review of all arguments presented by each position on which a consensus among international legal experts was ultimately reached in the course of a NATO-sponsored process, but also identification of those areas in which no consensus was found to be possible in the first edition of this work (2013, with a second edition expected in fall of 2016). Analysis of those areas upon which profound disagreements remained identified areas that are clearly vulnerabilities for the nature of the geopolitical state itself, with the concept of vulnerabilities referring to those challenges to a system that are capable of disrupting the system altogether, in contrast to sensitivities that may arise out of damage to a system the integrity of which is maintained. These vulnerabilities derive from and manifest tensions between the geopolitical and the network political. This paper will examine how those vulnerabilities are manifested and dealt with at the other end of processes that could unfold should cybersecurity problems become cyberwarfare and result in occupation of physical territory by analyzing the Tallinn Manual treatment of international law for occupation. The conclusion of the paper will provide an integrated analysis of manifestations of vulnerabilities of the nature of geopolitical state itself -- not just of individual states -- in disagreements about the applicability of existing international law to what we might call cyber-contexts. Governance Looking Out: Trade, Finance, and Territorialization

Mutual Legal Assistance in the Blended World of Political Space and Cyberspace

Peter Swire, Nancy J. and Lawrence P. Huang Professor in the Scheller College of Business at the Georgia Institute of Technology

Trans-border consumer services, such as for email and social networks, mean that the evidence in an increasing number of criminal prosecutions is held in another country, such as when a non-US crime involves records held by a US-based service provider. The regime of Mutual Legal Assistance Treaties operates at the speed of traditional national sovereign actions, often taking a year or more for evidence to be produced even when the legal standards are met. This talk will highlight findings from our ongoing research project on how to update Mutual Legal Assistance to cyberspace speed, for records that are pervasively held in cyberspace.

Capital Controls in the Age of Cryptocurrency

Eli Dourado and Caleb Watney

For a century, governments have used capital controls to make capital flows more predictable, defend the value of their currencies, and limit global economic competition. Although capital controls have lost intellectual favor since the 1970s, they have regained some support since the 2008 global financial crisis. Putting aside the normative policy considerations surrounding capital controls, on a positive level, there is reason to doubt that capital controls will continue to be an option governments can exercise in the future. Capital controls are enforceable because the vast majority of cross-border financial activity is funneled through a relatively small number of regulated bank intermediaries. As cryptocurrency technology matures, ordinary citizens gain the power to directly engage in cross-border payments without a regulated third-party intermediary. As a direct consequence, the cost of enforcing capital control policy may become prohibitive. In this paper, we review the mechanics of how capital controls are enforced today. Next, we show how Bitcoin and other cryptocurrencies undermine those enforcement mechanisms. Then we examine the limited and still unpersuasive evidence to date that cryptocurrencies are already affecting the ability of governments to impose and enforce capital controls. Finally, we discuss the future prospects for cryptocurrency to undermine capital controls, including likely government reactions and limiting factors.

Trade agreements and global freedom of information

Susan Ariel Aaronson, Elliott School of International Affairs, George Washington University

This paper focuses on the Trans-Pacific Partnership's (TPP) language on information flows, which can affect both trade and human rights. I examine four chapters of TPP—the services chapter (which delineates what kind of services are covered; e-commerce (which governs cross-border information flows), the transparency chapter (which regulates how governments provide information to their citizens and the exceptions chapter (which sets rules governing how and when nations may breach their obligations in the interest of public morals, national security, privacy and public health.) I show that these chapters may help netizens and policymakers advance internet openness and make it harder for officials to restrict information flows. I argue that TPP could play an important role in encouraging cross-border information flows and in providing tools to challenge censorship and filtering. Moreover, the agreement contains transparency requirements that could bring much needed sunshine, due process, and increased political participation to trade (and Internet related) policymaking in countries such as Malaysia. Nonetheless, TPP will not preserve or protect the open Internet unless policymakers use its provisions to challenge such restrictions.

Contact:
Karim Farhat

(404) 345-6222
karimfarhat@gatech.edu