SOVEREIGNTY, NATIONAL SECURITY, AND INTERNET GOVERNANCE

PROCEEDINGS OF A WORKSHOP

Organized by Milton L Mueller, Syracuse University School of Information Studies, and Hans Klein, Georgia Institute of Technology School of Public Policy, December 12, 2014

The Internet Governance Project

http://internetgovernance.org

Contents

Rationale for the workshop

Is cyberspace changing the nature of the state?

The workshop, held December 12, 2014 at Syracuse University's Lubin House, focused on the changing nature of the state and sovereignty. Informed and in many ways inspired by the work of Philip Bobbitt (2002, 2006) it brought together scholars of political science, international law, national security, and Internet governance to explore the question whether cyberspace is changing the nature of the state.

Theories of state sovereignty build on two fundamental distinctions: the distinction between internal and external sovereignty, and the distinction between the state and society (or the public and private domains.) These distinctions are being undermined by various trends, not least the global shift to digital communication technologies.

The Internet collapses space, as users around the world interact without regard for territory, engaging in cross-border exchanges and eliciting state actions that blur the domestic-foreign divide. Thus we see a US agency of national security (the NSA) protect against external threats by engaging in comprehensive domestic surveillance. And we see a US domestic policy response that posits privacy rights for all Internet users, even if they are outside US territory and are not US citizens. Likewise, the distinction between public and private domains is undermined by current trends. The Internet is composed of private networks, services, and application environments that in their totality create a public sphere of global communication.

This workshop fostered an intensive dialogue among a small, focused group that includes theorists of sovereignty, cyber-oriented international law experts, and cybersecurity and Internet governance experts. It engaged in a critical evaluation of the applicability of Bobbitt's ideas regarding the changing nature of sovereignty, drawing on experiences in the Internet sector generally and the NSA's practices in particular.

Milton Mueller
Hans Klein
February 19, 2015

Workshop participants

Philip Bobbitt, Columbia/Texas (International Law, History)

Jeremy Crampton, Kentucky (Political Geography)

Camille Francois, Harvard Berkman Center (Internet studies)

Jack Goldsmith, Harvard (International Law)

Hans Klein, Georgia Tech (Political Science)

Catherine Lotrionte, Georgetown (International Law)

Tim Maurer, New America Foundation OTI (Internet governance)

Milton Mueller, Syracuse (Internet governance)

Helen Nissenbaum, NYU (Internet studies)

Lou Pauly, Toronto (Political Science)

David Post, Temple (Law, Internet governance)

Wolf Schuenemann, Heidelberg (Political Science)

Sebastian Stier, Heidelberg (Political Science)

Peter Swire, Georgia Tech (Law, Policy, Ethics)

Session 1: Challenges to forms of the state

- Are traditional conceptions of sovereignty crumbling?
- Is the form of the state changing?

Discussion leaders: Philip Bobbitt and Jack Goldsmith

"The belief that we live in a Westphalian world and have been…since the 17th Century is a crippling mistake." – P. Bobbitt

Philip Bobbitt opened, noting that his book *The Shield of Achilles* was about the interrelation of strategy, law, and history. It was based on challenging three major "end of history" theories. Fukuyama's claim that there is a democratic-liberal consensus was shattered by Bosnia, which showed that such a consensus did not exist even in the center of Europe. Theories that saw globalization as a "virtuous cycle" collapsed on 9/11, as the dark side of globalization was revealed. And Huntington's idea of the "clash of civilizations" also did not work; e.g. in Iraq and Korea, it was struggles within cultures, not across them that led to conflict.

There is a grain of truth in each of these theories – all posit that we are at a pivotal moment in history. Yet all of these theories hold the state constant. None of them consider that the state itself, the constitutional order of the state, is in play. Yet it is in play, and that is what really makes things pivotal. And while we do still live in a world of nation-states, the belief that we live in a Westphalian world and have been in a Westphalian steady-state since the 17th Century is a crippling mistake.

Bobbitt then discussed the relationship between military strategy and the constitutional order in historical terms. The form of the state changes, each type of state is based on a different kind of "compact." For princely states, for example, the compact is: give us power, and we will protect perquisites of princes, mainly religion. As society evolves the compact changes. Bobbitt does not want to argue that military strategy always determines constitutions. They are interdependent. Sometimes technological changes that alter strategy drives constitutional change, but during the change from territorial states to imperial state-nations the reverse happened; constitutional changes and changes in the political context, such as mass conscription, changed the nature of warfare.

We are in a moment of change, but it is not a simple matter of nation-state dying and going away, nor is it a simple matter of the forces of change dissipating and the status quo remaining in place. We are changing because the industrial nation-state can no fulfill the compact upon which is it based. There are 5 reasons why it can longer deliver on its promise:

Session 1: Challenges to forms of the state

The early Internet debates seem very naïve now, including my own view. They did not appreciate the way a global network creates opportunities for state & nonstate actors to do mischief across borders. – Jack Goldsmith

1. Globalization of trade and finance means no state can manage its economy independently
2. Transnational threats such as AIDs, SARs, climate, terrorism
3. Internationalization of culture and communications
4. Development of WMD and their commodification
5. Development of a system of international law that supersedes national law

To meet these challenges, Bobbitt implies, a new constitutional order must be devised. Bobbitt dismisses declinist arguments about the West. They irritate him because it's all just foreplay. Declinists never seem to tell us to where the decline leads? Bobbitt has an answer: he believes a new constitutional order is emerging. When the state is faced with challenges, it innovates. If it does not, it is superseded by competing forms of the state.

Jack Goldsmith introduced the mainstream theories regarding sovereignty, based on Stephen D. Krasner's 1999 book *Sovereignty: Organized Hypocrisy*. Krasner distinguishes between 4 types of sovereignty:

1. International legal sovereignty, involving mutual recognition by other states with formal juridical independence;
2. Westphalian sovereignty, involving the exclusion of external actors from the authority structures in a territory; the exclusivity of the political institutions;
3. Domestic sovereignty, meaning the ability of public authorities to exercise effective control within their territory;
4. Interdependence sovereignty, meaning the ability of public authorities to regulate the flow of information, ideas, goods, people, capital, etc. into and out of their borders. (This obviously has important implications for #3, domestic sovereignty)

Is the idea of Westphalian sovereignty valid today? Has it ever been valid? Krasner's answer would be no. Westphalian sovereignty can be violated both by external intervention and by "invitation," i.e., when a ruler of a territory voluntarily agrees to compromise the domestic autonomy of the polity. Both Westphalian and international legal sovereignty have been violated routinely in history; neither has been a stable equilibrium from which no actor has an incentive to deviate. In Krasner's view, both concepts of sovereignty are best understood as "examples of organized hypocrisy" – rulers adhere to conventional norms of sovereignty when it offers them resources and support, and deviate when violating them provides benefits.

Globalization was supposed to undermine interdependence sovereignty. Here Goldsmith refers back to the Internet governance debate of the mid-1990s, noting that both he and workshop participant David Post were involved in it. That debate asked whether self-ordering or the state would (or should) control cyberspace. That debate, according to Goldsmith, seems very naïve now, including his own view. It did not fully appreciate the opportunities a global network

creates for state and nonstate actors to do mischief across borders. Cybercrime and the surveillance state both actualize this potential. A lot of people thought the Snowden revelations would weaken the surveillance state (e.g., by encouraging encryption). It may, but also creates new opportunities for the state. The NSA loves it when people shift to something they think is secure and it really isn't. The Snowden revelations have also led more states to seek control over communications in their territory, which is not going to be good for privacy.

Goldsmith thus agrees with Bobbitt that the state innovates. The State did a good job of taking advantage of the Internet to serve its own ends, but is changing as a result. The debate over the role of the state in cyberspace has suffered from the same fallacy identified by Bobbitt earlier: it tends to hold the state constant.

Discussion

Agreeing that we are witnessing the emergence of a new form of state, Louis Pauly noted that he and Edgar Grande (in *Complex Sovereignty*) proposed calling it 'the transnationally networked state inclined toward cooperation.' Noting a point long ago made by Robert Keohane, he distinguished 'cooperation' from 'harmony.' Inside the silo of the territorial state, he agreed that policymakers can't manage the fundamental problems Bobbitt identified. They really do have to find ways to cooperate across conventional territorial and treaty-constrained boundaries. But we are constantly confronted with the idea that they can. A conversation he had recently with someone from the MITRE Corporation provided an example of this: cybersecurity, the man claimed, requires rebuilding and fortifying the nation-state.

Catherine Lotrionte observed that the State is not 'coming back,' it never went away. The CIA was talking about information warfare as early as 1997. Westphalian treaties are based on the concept of freedom from external interference. By respecting states equally we reduce chaos in the international arena. She refers to the way the State Department is undermining of Chinese sovereignty through Internet freedom initiatives. Referring to Henry Kissinger's book *World Order*, she cautioned us to tread lightly in our interventions. She doesn't think the territorial state will ever go away.

At this point Bobbitt introduced the distinction, developed in his book *Terror and Consent*, between three different conceptions of sovereignty. *Opaque sovereignty* – the idea defended by Lotrionte – is the classical Westphalian model, wherein states are autonomous individuals with equal rights, and no other state can legitimately interfere with that autonomy no matter what goes on inside its borders. *Translucent sovereignty* means that the legality of acts of

sovereign states can be assessed by an authoritative international legal body whose purview penetrates the veil of national sovereignty. This view is associated with the European Union and the actions of the UN Security Council under the "responsibility to protect" doctrine. *Transparent sovereignty* locates the source of sovereignty in popular consent. Because the people cannot consent to a violation of their inalienable rights, transparent sovereignty empowers the international community to question the legitimacy of exercises of state power within their own borders. The latter concept is associated with Americans, who trace sovereignty to a different source than in Europe. In Europe, a state takes it sovereignty from its predecessor state; in America sovereignty is delegated to the state from the people. But **Wolf Schuenemann** challenged the American-ness of the concept, comparing transparent sovereignty to Habermas' concept of popular sovereignty.

Milton Mueller asked, do we need to discuss sovereignty per se? Is this notion central to what we are discussing, or is what really matters the change in the form of the state? Are shifts in the notion of sovereignty merely epiphenomena of changes in constitutional orders? I understand how the notion of popular sovereignty was associated with a change in the nature of the state, but am not clear how or whether other historical changes in constitutional orders were related to shifts in the practice of or ideas about sovereignty. **Bobbitt** agreed that the concept of sovereignty per se is a bit of a distraction. The concept arises from a European feudal environment, and refers to the ability of the prince to control his body; attributes of the individual are mapped on to princely states. Popular sovereignty on the other hand is a late 18th century concept. The concept of sovereignty per se is not the important element here, it is a derivative of the truly important thing, which is the devolution of power to individuals and small groups.

Society is adapting to the new power opportunities presented by cyberspace, **Camille Francois** claimed. In this adaptation there are two distinct threads; one explores more distributed models of governance, the other focuses on security and cyberwar within the nation-state paradigm. But these two threads have never intersected, they just continue on in parallel. **Peter Swire** agreed. A military has to be world class at offensive and defensive cyber, he said. Cyber capabilities have been pushed down to the platoon level in the military. Military interest in cyber won't go away and can't go away if you are going to be responsible. But he agrees with Francois that the gap between these military developments and the more distributed models of governance exists, and the two strands need to be reconciled.

Session 1: Challenges to forms of the state

Addressing Bobbitt, **Hans Klein** asked: to explain the present, you went back 500 years. Can we come up with deeper insights about tectonic shifts in the nature of the state from this retrospective view? What stays constant and what changes? Is it the monopoly on violence? It doesn't seem to be territory. Or is it legitimacy that changes? *Legitimacy is what stays constant*, **Bobbitt** replied. Every legitimate power is based on a compact. Give me power because…. A state loses legitimacy when it cannot deliver on its promise. Every society is constituted in some way. The State-nation says give us power and we will forge the identity of the nation, fuse it with the state. Each constitutional order creates its own kind of international order. In Bobbitt's view, peace congresses that resolve epochal wars write constitutions for international order.

Louis Pauly noted that political scientists distinguish between *Power* and *Authority*. Authority involves a mutually recognized right for an actor to engage in certain kinds of activities; power or control means the ability to compel action. One can have control without authority. But if power cannot solve the problems it is confronted with, it has no legitimacy. And if coercive power is to be used to address problems, it must have legitimacy. This line of discussion reminded **Lotrionte** of the McDougall/Lasswell criteria of whether international law is law. If international law is law, then one must look at whether the norms are both authoritative (accepted as legitimate) and controlling (affect behavior). Kosovo was illegal under international law, but widely accepted as legitimate. Legitimacy and legality – both are important. On the issue of security, Lotrionte noted that non-state actors (e.g., Wickr, Snapchat, Silent Circle) are using encryption to counter surveillance. She supports this – it increases the level of innovation and improves the security of communication systems. Let the smart guys do what they want to be more secure, and let governments try to work around it. American companies will be the leaders in this process.

Tim Maurer noted that Weber did not just refer to a monopoly on force but to a monopoly on the *legitimate* use of force. Legitimacy is also what got him thinking about surveillance and regime stablity. In the classic view of political scientists like Karl Deutsch, authoritarian regimes are less responsive to their citizens' concerns, and thus are more likely to be unstable and to suffer from legitimacy deficits. But he is concerned that modern surveillance technology might allow authoritarian governments to be more responsive, and thus more stable. **Wolf Schuenemann** related the discussion to Weber's different types of legitimate rule or rein: the traditional, the legal, the charismatic. Schuenemann also asked whether the market state is still bound to territory, to a legitimating nation.

"ICANN is a regulatory agency and as such should be subordinate to popular authority" – Hans Klein

Session 2: The case of Internet governance

- Does the globalized virtual space created by the Internet transform the nature of the state?
- Will the Internet's governance and architecture realign with national borders (or has it already done so)?
- To what extent is the interplay between national security and cyber vulnerabilities driving changes in Internet governance?

Discussion leaders: Hans Klein and Milton Mueller

Hans Klein opened the session. Beginning with a definition of the internet, he noted that it exists only at the software or logical layer (the TCP/IP standards) and does not include all forms of electronic communication. As a catalyst of change, we can distinguish two dimensions of the Internet: the way it reflects change in the relationship between *state and society*, and the way it reflects changes in *inter-state relations*.

With respect to the state-society relationship, ICANN is a regulatory agency. It picks winners and losers among applicants for new top level domains; it must take a stance on sensitive policy issues like pornography (the .XXX domain), and it regulates registrars and registries via contract. As a regulatory agency, ICANN should be subordinated to popular authority. It is so subordinated, in part, through its contract with the US government. On the other hand, it is also meant to be a private corporation and not subject to direct government control. In this view it should be an autonomous, quasi-sovereign entity. There has been a push to make ICANN more independent of the U.S., with no higher authority under contract or law. Here we see significant change in the state-society relationship. Just as independent regulatory agencies constituted a major change in the nature of the U.S. government, ICANN can be seen as a recognizable change in the nature of the state.

With regard to the inter-state dimension of Internet governance, Klein examined how the US-ICANN- complex relates to other sovereign states in the world. There are basically three different answers one can give to the question of who has supreme authority over the global domain name system: 1) ICANN itself; 2) the US government; 3) all the national governments of the world. The International Telecommunication Union (ITU) is an example of the third, intergovernmental option. Because the US is just one sovereign among many, using the ITU would solve the problem of constituting legitimate political authority over ICANN.

Session 2: The case of Internet governance

In US, the IANA transition (the attempt to end U.S. control of ICANN in favor of nongovernmental 'multistakeholder' oversight) has triggered a divisive debate. Some see the US as a market state supporting nongovernmental governance institutions; others see the US as a nation state, with national security and other interests that should be upheld in a realist way for its own national interest.

Milton Mueller wanted the discussion of Internet to look above and beyond ICANN. He came to the conclusion that the Internet is part of some broader transformation of the state while studying the revolution in telecommunications policy in the 1980s. Observing the AT&T breakup and the introduction of privatization, competition and deregulation in Europe and Japan, he became curious about the historical origins of the Post, Telephone and Telegraph (PTT) monopolies. He found that the modern postal monopoly was closely correlated with the rise of the territorial state in the 17th century. The state postal system not only provided secure internal communication for the state, it also gave the central government more control over the circulation of printed and written communications by society as a whole, helping it to secure political and military control of its territory during the turbulence of the Reformation and the 30 Years War. In Cromwell's England it also served as the basis for the first modern national intelligence agency (correspondence was brought into a central hub and opened for surveillance) and the modern newspaper (local postmasters collected 'news' from correspondence and compiled it into publications at fixed regular intervals in order to keep current with events). There was thus a clear connection between the ability to control communications and the sovereignty of the state. Telephone and telegraph technologies were simply taken over by the 17th century postal monopoly as a matter of course.

To see such a sudden and radical departure from the monopoly PTT in the 1980s and 1990s indicated to Mueller that something fundamental about the state was changing. The Internet was merely an outgrowth of this process; once liberalization opened the door to global market forces, innovation, new entry and competition, it also became possible for new so-called 'value-added services' or information services to ride on top of the physical infrastructure, and create a globalized virtual information economy with minimal entry barriers.

The rise of the Internet also produced a demand for some sort of globalized governance. This in turn led to contention among states, private actors and civil society over control of that globalized governance. ICANN is the focus of that debate only because it is a tangible, globally centralized institution. Other sites of Internet governance – such as content take-downs by

Session 2: The case of Internet governance

The sudden, radical departure from monopoly PTTs in the 1980s and 1990s shows that something fundamental about the state was changing – Milton Mueller

social media providers or interconnection agreements among ISPs – are decentralized and less transparent, and so elude debate.

Through the happy accident of "permissionless innovation," the Internet has demonstrated the value of communication and information flows that ignore jurisdictions. The Clinton Administration's 1996 Global Framework for Electronic Commerce sought to protect this emergent regime, calling for an order based on private contract so as to transcend jurisdiction. The state is no longer supreme authority over information. The only major tether to the old state system is the US IANA contract with ICANN, which is on its way out. Although the Governmental Advisory Committee in ICANN has become more powerful, so far states have been held at bay; their opinions are advisory; there are no governments on the board; there is little support to push the ICANN regime into the ITU or UN.

There are, however, disturbing signs of reversion to the nation state model. Nationalist conservatives in the U.S. resist the IANA transition. National cyber-security policies link Internet governance to nationally-bound policies. Free trade in telecom equipment comes to be seen as a security threat, triggering nationalistic chain reactions (U.S. fingers Huawei as a possible cyber-espionage threat, then China harasses Cisco and Microsoft). The Snowden revelations encourage attempts to reassert jurisdiction over information flows and also show how NSA have indeed exploited or produced vulnerabilities in equipment and standards to the advantage of one nation-state.

Discussion

Jack Goldsmith began the discussion by asserting that ICANN is more complicated than Klein and Mueller have indicated. It is not just a U.S. corporation but a California corporation, governed by California law. If the U.S. government goes away entirely, it might be possible for the California Attorney General to start manipulating global internet governance. This led to a discussion of whether ICANN's grounding in California corporation law is different from its tie to the U.S. federal government via the IANA contract, and whether ICANN could be more or less independent depending on where its jurisdiction is. Goldsmith didn't think sovereignty is a useful term for describing ICANN's decision making. ICANN was overturned on .xxx, was that an exercise of sovereignty? We need to have a real crisis and confrontation before we can know who is sovereign (Someone asked, referring to Jon Postel's attempt to redirect the root servers, didn't we have this confrontation?)

Session 2: The case of Internet governance

Goldsmith asked for a more systematic exploration of the threat of reasserting national borders. We need to tally the costs and benefits of letting local authorities have more control over the internet, he said. **Milton Mueller** and **David Post** replied by attacking the trend toward nationally fragmented communications. Not only does it empower censors and interfere with free trade in information services, it also allows states to project their authority beyond their borders illegitimately. The European regulations on the right to be forgotten, for example, could easily become global restrictions on free expression, requiring the removal of information or the blocking of search engine access in ways that are global instead of local.

Post also challenged Klein's idea that our only choices for supreme authority were ICANN itself, the U.S. government, or intergovernmental agencies. Who was the supreme authority over the Internet Engineering Task Force (IETF), which develops voluntary standards for Internet protocols? Reasserting the notion of popular sovereignty, Post said that the list of possible sovereigns has to include the community ICANN is intended to serve. **Hans Klein** then noted that the original institutional design of ICANN included an individual membership and global elections for half the board. This proto-democratic system was overthrown by the 'Ghana coup' (the poorly attended ICANN meeting in Accra when membership was abolished by the board).

Wolf Schuenemann said that technocratic governance based on and legitimated by expertise might work. As Europeans, he said, we have some experience with international technocratic governance that has developed for several decades under what neo-functionalists call permissive consensus. Referring to **Hans Klein's** claim that ICANN cannot have legitimacy, Schuenemann said this is not necessarily the case. Expert agencies can have a lot of output legitimacy at least in so-called low politics. What you see in the European example is that everything gets complicated when it comes to high politics or politicization. When do we step over into high politics, there was always the shadow of hierarchy.

Peter Swire noted that independent regulatory agencies, whose legitimacy is also based on expertise, are not even supposed to exist in some theories of government; formalists say everything has to be part of the executive, the legislative or the judicial branch. But we have had them since before the New Deal (1930s) and they don't fit into any of those categories. Another possibility is that legitimation comes from 'facts on the ground.' This kind of *de facto* control played a big role in the early stages of Internet governance, **Mueller** affirmed, because of the way the Internet was an emergent phenomenon that evolved from nonstate actor communities with authority over Internet resources.

Session 2: The case of Internet governance

Here **Louis Pauly** brought up the financial crisis as an illustration of the relationship between public and private authority. We are moving deeper and deeper into what Keohane and Nye called “complex interdependence.” We want to get past the next constitutional moment without the bloodshed of an epochal war. This requires dealing with the unintended consequences of deeper interdependence. Private authority is an American idea to obfuscate the issue. There is a sort of output legitimacy, but, as we saw in 2008, in crisis situations the state comes out of the closet and manages the crisis. Then it returns into the closet and everybody forgets about it very quickly. We can’t see where the coercive authority is. But if it isn’t there at the moment of crisis, the system collapses.

The discussion then moved to the third area, regarding the role of cyber ‘war’ and vulnerabilities in driving changes in strategy and governance. **Catherine Lotrionte** initially asserted that traditional state capabilities are simply adapting to the new threats without major changes in constitutional order or in international law. There is already an international law of armed conflict (LOAC). The US position is that LOAC applies to cyberspace. So does the UN Charter’s definitions and rules regarding the use of force. If there are ambiguities in figuring out how to apply these rules to cyber, the Tallinn Manual is starting to work this out. Decisions about what counts as acts of war are made only by states; but international law can be applied to non-state actors. Lotrionte recognizes that attribution is still a problem, but capabilities seem to be getting better; e.g., reliable sources indicate that the Sony breach was state-backed. She also emphasized the importance of all-source intelligence to attribution; one should not just use cyber sources for cyber attribution.

Camille Francois asked whether cyber capabilities were actually creating a new layer of norms that are more escalatory than in other domains, and that its intersection with these other domains might disrupt the peace equilibrium. How do cyber-attacks, for example, intersect with nuclear weapons? Different norms can create instability and new opportunities for escalation. In response, **Lotrionte** had to admit that cyber capabilities are changing the international equilibrium. The UN has formed a Group of Governmental Experts (GGE), which now involves 20 states. The French want to discuss a new norm for taking critical infrastructure off the table for cyberattacks during peacetime – that would be a change in international law. Hospitals and financial systems should also be off the table. China and Russia want new treaties around cybersecurity, but their approach emphasizes sovereignty and counts censoring ‘subversive’ content as part of cybersecurity. It is still tricky to define what counts as an armed attack; in fact, this will be worked out through state practice and by what states say after an event. Disagreements in the international community will lead to pushback; maybe in the future these

issues will go to the UN Security Council. Also, it is harder to monitor the development of cyber weapons than nuclear or other kinetic weapons. Some say the established rules of engagement can be applied to cyber warfare, some say new rules of engagement must be developed. But, she concluded, the state will not go away in security issues.

There is no doubt we remain in the state-centric world, **Louis Pauly** replied. But there are two kinds of states: Bobbitt's market states and nation-states. The US is trying to encourage the transformation of China into a market state. In the past, such transformations occurred in the wake of wars. Can it happen today without a catastrophic war?

We need to be looking towards a transformation of International law that governs relations between market states. **Philip Bobbitt** noted that while there may be existing institutions into which we can throw these problems, it is unclear whether they can effectively deal with them, or with decentralized threats coming from non-state actors. States are organized to pursue their national interests rather than global or transnational interests.

Helen Nissenbaum observed that the techies she knows at NYU were most worried about the cyber-criminal constituency. Some of the criminal actors may be able to multiply their power such that they can escape the control of the state actors. International law will not affect those sorts of actors. **Bobbitt** added that such actors can also play one state off against another. **Lotrionte** replied that China hasn't signed the Budapest Convention on Cybercrime but thinks it has a problem with cybercrime too, so China is willing to work together. There is the possibility of joint takedowns, and strengthened MLATs. She cited the Microsoft takedowns and cooperating with private sector in this process. But **Peter Swire** noted that Microsoft was able to grab American data in Ireland; if we do that, will China want to do the same thing? Extraterritoriality can happen in this area too.

Session 3: The case of surveillance

"PPD28 says that we shall afford non-U.S. nationals privacy rights. This is a major change in the history of espionage." – Peter Swire

- How globalized has surveillance become due to the prevalence of cyberspace?
- Is mass surveillance justified by the need for pre-emptive actions against terrorism, WMD proliferation, etc.?
- How are cooperation and contestation among states over cyber-surveillance contributing to the evolution of new forms of the state?

Discussion leaders: Peter Swire and Jeremy Crampton

Peter Swire served on the President's Review Group on Intelligence and Communications Technologies. His task was to provide advice that gave due weight to the problems of national security, international economic relations, privacy, civil liberties, trust and insider threats. The US policy goal is an open, interoperable, secure and reliable internet. The intelligence community should not govern the internet. Before stockpiling Zero-day exploits or collecting massive amounts of data, the White House, Commerce and State Departments should also get involved so that policy objectives other than purely military/intel ones can be taken into account.

Regarding globalization, Swire noted that consumer protection law has for a long time dealt with the problem of whether the applicable law should be from the place of the company or the place of the consumer. Companies tend to support the former view; European peoples and states tend to support the latter view. Through private contract, global American Internet companies have worked out ways to make sovereignty not matter very much. However, when trans-jurisdictional law enforcement issues arise, the rest of the world has to come to Mountain View (California) or Redmond (Washington) to get criminal evidence. This is long and troublesome for them.

Regarding the third question above, Swire noted that Presidential Policy Directive 28 (PPD 28, "Signals Intelligence Activities," January 17, 2014) says we that we shall treat foreigners as people. Non-US nationals are afforded privacy rights, and minimization rules are supposed to apply to them. This is a major change in the history of espionage. Swire noted that we want to avoid a war of all against all on the Internet. How can we build areas of cooperation even when values vary? He supports development of confidence-building and step-by-step measures for cybersecurity, such as norms against attacks on critical infrastructure or financial systems. We need to link the discourses on cybersecurity based in the military, intelligence and law

enforcement communities with the values of the traditional Internet domain (distributed, bottom-up, civil society based).

Jeremy Crampton began his talk by posing four questions:

1. Google is surveilling people. Is this a new form of sovereignty? Is it the state rolling back, or is it the state extending its capabilities through outsourcing and contracting? When are the activities of a Google or Facebook state activities?
2. Regarding geo-surveillance, locational data is problematic from a privacy point of view but it is also an object of value that is becoming monetized. Geo-surveillance provides activity-based intelligence. From an intelligence perspective, tracking individuals is not as relevant as tracking groups. How does this transactional surveillance affect how we understand space?
3. Cyber warfare. What is the role of non-state actors? According to Sean Harris' new book (*@War: the Rise of the Military-Internet Complex*) private corporations are equal to or ahead of government in their cybersecurity capabilities.
4. How are people constituted as subjects of surveillance? In the book *1984*, you knew you were under surveillance and adjusted to it. Now, we are inured to it. Algorithmic surveillance, big data; smart cities, Internet of Things; big data raises questions about how people's behavior is affected, and it becomes a bigger deal as all the data streams become interoperable.

Hans Klein asked whether it was novel ground for PPD 28 to recognize non-US persons. According to **Catherine Lotriionte,** PPD 28 was just a recommendation. It does not change Executive Order 12333, which is where the U.S. government defined a US person. Whether collection takes place inside or outside of the USA is a much hairier issue, however. But there won't be any change in what the intelligence community is doing unless 12333 is changed. **David Post** said that PPD-28 sounds like a potentially big deal; a wedge for change. Although it applies only to intelligence activities, the principle behind it is relevant to other internet governance battles. During the legislative fight over SOPA/PIPA, one objection was the way it denied due process to foreign infringing websites.

Milton Mueller noted that the Harris book on U.S. cyber military expressed disappointment in the limited nature of the Obama administration's NSA reforms. It seems to be difficult if not impossible for states to give up capabilities that give them a power advantage. Still, we do see some pressure to globalize privacy rights in the U.S. What about other countries, especially western allies of the USA who are complaining about the NSA? Are they moving in the same direction? **Swire** replied that he was not aware of any movement there. Camille Francois added that it is hard for expats to figure out when they are protected by privacy laws and when

not; terms of service, which services to use; regionalized services; it is as complex as a three-dimensional chess game.

The Idea that the corporation is disembedded from the state is wrong, **Pauly** insisted. That Google, Microsoft, Intel, and Coca-Cola, for example, are American corporations remains meaningful. Certainly that fact and its implications are well understood outside the United States. Nevertheless, we are currently experimenting with another way forward. Pauly's book, *Who Elected the Bankers?* set out one example. In the mid-1970s, in the context of negotiations over international monetary reform, the U.S. accepted an obligation to submit itself to surveillance by the IMF. In 1944, at Bretton Woods, the U.S. would not accept such an infringement on its sovereignty. In 1975, the U.S. and other leading states accepted an obligation to account to their peers on the external effects of their policies. The U.S. accepted it because it wanted to extend the rule of law and thought it would benefit from the reciprocity of other states. But it, and other states, remained 'politically responsible' only to their own citizens. The U.S. moved from idea that you either have sovereignty or you don't, to a more nuanced, even 'European' idea that sovereignty is negotiable. Something similar in the cyber world could happen. We are accountable to international community, but we may have to do some things with the data because of our responsibility to our own citizens. In this new kind of state, sovereignty is indeed negotiable. Yes, we barter sovereignty, **Bobbitt** claimed: if you want to join the EU, for example, you have to give up capital punishment. Markets in sovereignty are a new thing in the postwar period. The content of criminal sanctions are not normally negotiated. **Goldsmith** countered that this is not new, all treaties are bargains.

Tim Maurer asked Swire about the Review Groups' recommendation on 'dual-hattedness,' i.e., the head of the NSA also being head of Cyber Command. **Swire** replied that NSA should act as an intelligence agency, not a war fighter. Cyber Command is not well-staffed, it is still learning how to do things. Consequently, its ability to stand apart from the NSA is limited. Still, the offensive and defensive side should be split. Who will trust us to do defense when the same folks are doing offense? However, he recognizes that the 'people who do this stuff' say if you want to learn how to defend you need to know how to attack.

Addressing one of the Review Group reforms calling for having a 3rd party in the Federal Intelligence Surveillance Court room, Catherine Lotrionte claimed that this might inhibit honesty between judges and lawyers. The military officers would self-regulate what they said. **Goldsmith** replied that that chumminess is exactly what was wrong with current system; we need a more adversarial approach. **Swire** added that after 9/11 FISA review is more about

approving whole programs than the surveillance of an individual person. The need for adversarial argument comes with more programmatic intelligence-gathering initiatives that create secret law that affect millions of people.

Helen Nissenbaum: Most of my work focuses on private actors (behavioral advertising). She rejects the "so what, it's just advertising" argument. Seems like killing a fly with a sledgehammer – we are creating a massive surveillance infrastructure for this little ad. Even though the infrastructure is in private hands, doesn't this make us vulnerable to state actors coming in and utilizing it? Peter Swire noted that private companies have pushed back hard against misappropriation of their data gathering by encrypting everything. They want to make their domestic and foreign customers feel secure, otherwise they will lose business. But government could still get things surreptitiously, or through court order. Jack **Goldsmith** noted that surveillance used to be a lot more targeted. New technology for bulk collection is what makes this problem arise.

Nissenbaum challenged the idea that it is better to constrain the *use* of data rather than control its collection. We can't stop information from circulating once it's collected. Bobbitt held that it is easier to constrain use. You might not be able to stop me from taking pictures, but you can stop me from publishing them or selling them. Something changes when the data is captured, **Nissenbaum** replied and **Peter Swire** agreed that we don't know what will happen to the data. If the government changes, if it becomes an authoritarian state, it could be misused. **Bobbitt** didn't like that argument. You are saying that building capabilities that could be used by a police state moves us closer to a police state – but that would prevent us from having guns or police departments. **Schuenemann** noted that Germany has nevertheless moved in the direction suggested by Nissenbaum and Swire. Legislative restrictions on the German intelligence service used to be about how the data was used, now it focuses on collection. Where does it lead society, he asked, if everything is archived? Any precautionary principle argument is about balance, Bobbitt replied. While data collection can degrade the human experience, it's not sufficient to stop there. We have to agree on what the harm is. Is the collection by machine so troublesome and provocative that we want to eradicate it, knowing that there will be occasions when we will need the data? **Camille Francois** asked if we **c**an ensure the security of this information from bad actors. Big data leads to the risk of big data breaches.

Hans Klein noted the strange duality of the U.S. state. Google and Yahoo are the darlings of the U.S. market state; they are wealthy and renowned brands. At the same time they are being

Session 3: The case of surveillance

attacked as enemies of the U.S. security state because of their moves toward using encryption. Are they the big surveillance threat or are they the chief resistors to it? **Swire** responded by emphasizing the economic pressures these companies face: there is huge growth in the global market and they may miss out on it due to surveillance-inspired mistrust. The companies and the U.S. Commerce Department don't want to handicap the companies, but the FBI director is not so happy with their use of encryption. **Jack Goldsmith** elaborated on the duality: If it is data for cybersecurity, they say 'yay, information sharing!' If it's information sharing for surveillance, they say 'boo, you're in the pocket of the NSA.' But Sony sure wanted the FBI to be there when they were hacked; Google wanted the NSA around when they had trouble with China.

Session 4: Possible new forms of the state

"The military, the intelligence agencies and the taxing authorities are the hard core of the state. Can we expect more breaches in the hard core of sovereignty? I think we can." - Louis Pauly

- Is Bobbitt's 'market-state' or 'state of consent' an adequate conceptualization of the changes underway?
- What are some alternative conceptualizations of sovereignty?
- Complex sovereignty, transparent sovereignty and other new conceptions of sovereignty

Discussion leaders: Philip Bobbitt and Louis Pauly

Philip Bobbitt returned to the idea of the *compact* to differentiate the market state from the industrial nation-state. The industrial nation-state said: give us power and we will improve your material well-being. Market-states say give us power and we will maximize your opportunities. Such states use the market rather than trying to defy it, they bend it to their own purposes. Market states are not good at family, reverence for sacrifice and other non-market values. Reproductive freedom, relaxed immigration and the all-volunteer army are examples of market-state phenomena. Market states are neither left nor right. They are more agnostic, more amenable to pluralism and multiculturalism. If you want to promote specific cultural values or identities you have to form your own civic associations to do so. The European Union was cited as an innovative example of an emerging market state.

Louis Pauly again stated that his book with Edgar Grande addressed the same issues as Bobbitt, but asserted that Bobbitt did it earlier, more convincingly, and certainly more elegantly. A second volume of his work along this line is tentatively entitled "Governing Global Risks." Cyber is opening up a whole new world of risk. Pauly is interested in the contemporary period of transformation. The military, the intelligence agencies and the taxing authorities are the hard core of the state. Can we expect more breaches in the hard core of sovereignty? He thinks we can, and we must recognize that they are vitally important if global risks are to be managed.

The distinction between internal and external sovereignty is important here. Internal sovereignty refers to the state/society relationship, external sovereignty refers to the relationship of the state to other states. Sovereignty can be divided and transformed without losing its substance. This idea is one of the most important innovations in modern political philosophy. The absolutist state concentrated or consolidated sovereignty, the nation-state led to the integration of populations in a territory. In the contemporary era we are learning that territory can open up, and the demos can open up.

Pauly then outlined some of the transnational risks and the challenges they posed to the state. In the wake of 9-11, Americans did much to militarize the U.S. – Canada border. The effort was futile. Certainly any imaginable security threats emanating from north of the 49th parallel can really only be reliably identified and contained with the cooperation of Canadian authorities. He hopes the he U.S. and Canada have now developed a more integrated approach, for it is in their mutual and long-run interest. The isolated state can't even guarantee basic personal security to its citizens, certainly not at any reasonable economic cost. Canada certainly rediscovered this during the SARS crisis, when the U.S. Center for Disease Control played a crucial global role. The U.S. Treasury and Federal Reserve did the same in 2008, despite what can be imagined as initial reluctance, even from the then-Treasury Secretary and a Republican president dedicated to free-market principles. At the moment of emergency, U.S. taxpayer resources were used to bail out American and foreign financial institutions.

Can the global systemic-risk management role of the United States be counted on in the future? Can key leader and follower states be counted upon to make mutual and mutually self-interested policy adjustments? Will what David Lake has described as a functional hierarchy of power remain durable? Those critically important questions open to doubt and debate as political and economic power becomes more widely distributed. Pauly noted that Lyndon Johnson's presidential program was labelled "the great society." The equivalent aspiration today, he contended, would have to have a serious global dimension. The "market," as in Bobbitt's "market state," remains a key instrument of policy, but it needs deeply rooted social foundations, which can no longer be entirely bounded by territorial limits.

Discussion

Milton Mueller asked whether the definition of the market state was robust enough. Is the concept linked to the growing scale of economic, political and social organization? Is the EU itself a market state or are the individual countries within it the market states? China is clearly not a market state, but rather a traditional industrializing nation-state. One of the oddest things about *Terror and Consent* was that Bobbitt called Al Qaeda a market state, too. States of terror are also market states?

The EU is the market state, **Bobbitt** replied, but it's not an inevitable historical progression to the market state. The single currency will be a catastrophe because it cannot easily coexist with nationally-determined budgets and fiscal policies; trade imbalances will crush country after country in Europe, leading to a more nationalistic politics. China is now a part of the hierarchy of powers, it won't destabilize the system. Regarding Al Qaeda, Bobbitt clarified that it has an

army, welfare programs and declares wars, so he wanted to call it a state. (ISIL might be a better example now.) It is transnational and it maximizes opportunity for Islamists whose main concern is to go to heaven. Al Qaeda is insurgent against the Western powers because they believe exposure to western culture has undermined their ability to maximize its subjects' opportunity to go to heaven. The globalizing market state does threaten some states. Very powerful states can become insurgent states.

Helen Nissenbaum asked whether states use the market or the market actors are using states. This led to a discussion of the growing tensions between nation-state regulations and the multinational Internet companies and whether this was leading toward 'fragmentation' or 'balkanization' of the Internet. **Peter Swire** noted that on the day of this conference Google had pulled its engineers out of Russia and shut down Google news in Spain because of new regulations regarding copyright payments. **Tim Maurer** called attention to the broader protectionist reaction against Internet companies in Europe, such as the European Parliament's call for splitting up Google. Network effects led to market dominance, a galling fact for the Europeans, but positive network externalities would only be diminished if the network leader is split up. **Nissenbaum** and others predicted that Spain would back down in this confrontation. Mueller noted that many of the anti-Google initiatives were simply responses to lobbying by old media companies who were threated. But this kind of reaction seems inevitable as long as the territorial scope of political authority clashes with the transnational Internet. Pauly had spoken of opening up the demos, Mueller noted. Why can't we see the Internet community as a new demos at least for governing the Internet? Could a transnational political community be the only solution to the fragmentary pressures? **David Post** amplified this point. Referring to Jefferson's Notes on the State of Virginia, Post said that in the 18th century no one could imagine scaling democracy up to a continental scale. While it may be similarly inconceivable today to imagine a global Internet polity, we did eventually get a continental scaling up of democracy.

Philip Bobbitt ended the session by reading *Perhaps*, a poem by Shu-Ting

Perhaps these thoughts of ours
will never find an audience
Perhaps the mistaken road
will end in a mistake
Perhaps the lamps we light one at a time
will be blown out, one at a time

Session 4: Possible new forms of the state

Perhaps the candles of our lives will gutter out
without lighting a fire to warm us

Perhaps when all the tears have been shed
the earth will be more fertile
Perhaps when we sing praises to the sun
the sun will praise us in return
Perhaps these heavy burdens
will strengthen our philosophy
Perhaps when we weep for those in misery
we must be silent about miseries of our own

Perhaps
Because of our irresistible mission
We have no choice

Books and articles referenced

Bobbitt, P. *The Shield of Achilles: War, Peace and the Course of History*. New York: Anchor Books (2002).

Bobbitt, P. *Terror and Consent: The Wars for the 21st Century*. New York: Knopf (2008).

Grande, E. and Pauly, L. *Complex Sovereignty: Reconstituting Political Authority in the 21st Century.* Toronto: University of Toronto Press (2005).

Harris, S. *@War: the Rise of the Military-Internet Complex*. New York: Harcourt (2014).

Jackson, R. *Sovereignty*. London: Polity Press (2007).

Kissinger, H. *World Order.* New York: Penguin (2014).

Krasner, S. *Sovereignty: Organized Hypocrisy*. Princeton University Press (1999).

McDougal, M., Lasswell, H., Reisman, W. Theories about International Law: Prologue to a Configurative Jurisprudence, 8 *Virginia Journal of International Law* 188 (1968)

Mueller, M. *Networks and States: The Global Politics of Internet Governance*. Cambridge: MIT Press (2010)

Mueller, M. *Are we in a Digital Cold War?* (May 2013) Retrieved from Internet Governance Project: http://www.internetgovernance.org/wordpress/wp-content/uploads/DigitalColdWar31.pdf

Pauly, L. *Who Elected the Bankers: Surviellance and Control in the World Economy*. Ithaca, NY: Cornell University Press (1997)

Post, D. *In Search of Jefferson's Moose: Notes on the State of Cyberspace*. Oxford: Oxford University Press (2009).

Swire, et al. *Liberty and Security in a Changing World: Report of the President's Review Group on Intelligence and Communications Technologies.* (12 December 2013) http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf