Internet Sovereignty
Sanjay Goel

Our world today revolves around the Internet, and anything that threatens its functioning causes worry around the globe. However, as we have seen, there are threats in the real world that far outstrip the intensity of any threat to, or on, the Internet. In my talk today, I will mainly comment on sovereignty and the Internet, and the implications for its ongoing operation, as well as for crime, warfare, society, and political order.

1. THE PROBLEM

The Internet is a shared resource among nations, and a powerful communication medium with a deep social and political influence. Nation states obviously have a strong stake in ensuring that social and cultural values are preserved, and political stability is protected. Countries are expected to follow established international norms, including respecting each other's sovereignty and territorial integrity, and non-interference in other countries' internal affairs. Despite these international norms, countries still engage in psychological warfare through propaganda (Fielding & Cobain, 2011). The spreading of propaganda across borders has been a State pastime for generations – now the Internet provides unprecedented means and reach to influence other countries' internal affairs.

The Internet was initially created for the free exchange of ideas and information among people. No one realized that it would become as powerful a force as it is today, with the ability to transform societies, trigger revolutions, and unseat rulers. It has surpassed newspaper, radio, and television in reach and usage; become a hub for commerce and banking, as well as a major venue for societal interactions. Since the scale, scope, and mandate for the Internet has changed so drastically, this may be a good time to reevaluate some of the fundamental assumptions that underlie its operations.

A de facto assumption of the Internet is that there are no borders; yet this is coming under increased scrutiny. Given the historic role of governments and nation states in maintaining territorial integrity, and in ensuring stability, the concept of unfettered borders is anathema. Is there a dichotomy between Internet borders and state borders? Conceptually, yes, but that dichotomy is increasingly seen as neither sustainable nor wise, and it was just a matter of time before fences were erected on the Internet. The technology for creating these barriers has existed and been demonstrated, but more universal acceptance and political will for barriers are slowly emerging across nation states. States that initially exerted control—China, Russia, and India—were criticized harshly for trampling on the rights of Internet users, and destroying the Internet's basic premise of freedom of speech without fear of repercussions. Death knells for the Internet in its current form were rung; predictions that the Internet would fragment into pieces were rampant. However, despite some barriers and controls being erected in multiple countries, the Internet is alive and well.

Nation states are anxious about information originating from the Internet that could be deleterious to their political stability and harmful to their citizens. The impacts feared vary from country to country -- from terrorist propaganda that leads to the radicalization of youth, politically sensitive propaganda that can cause uprisings, to sexually explicit material that will lead to exploitation and moral corruption. The propaganda may originate from outside, or from inimical elements within a country's borders. This has become a challenge for security and intelligence agencies. Countries today are as much at risk of instability from domestic actors as they are from external actors, and many, particularly the more authoritarian regimes, do not want to exacerbate internal problems further with external intervention (via the Internet).

Some countries have attempted unsuccessfully to shut down the Internet to quell unrest, as we witnessed in the aftermath of the triumphant democratic revolutions in Middle Eastern and North African countries that were at least partly facilitated by the social media. Protestors, particularly in Tunisia and Egypt, were able to use social media effectively, but state forces in Syria, Iraq and Libya quickly countered such protestor efforts. In the aftermath of the Arab Spring revolutions, governments are essentially on notice that the Internet functions as a global critic, and that they will need to keep their populations relatively satisfied to be able to rule. Given the potential of social media in influencing public opinion and organizing protests, countries could use social media as a weapon to foment unrest and overthrow governments of enemy countries and to impose their own system of government and society them. This is neither warranted nor successful as we have witnessed in the aftermath of the social media-facilitated revolutions in Middle Eastern and North African countries. In the power vacuum of unsuccessful outside intervention and civil unrest, we've seen terrorist groups such as ISIS, with its atrocities now well documented, rise, with the world reeling under a spate of attacks on innocent citizens.

Intelligence agencies around the world are now aggressively monitoring social media for political trends and attempting to address it via counterpropaganda, coercion, and censorship. The challenge that countries face is in keeping a reasonable balance between control and civil liberties so effective governance can be managed (Brown and Kroff, 2015). Clearly the Internet is a powerful global resource and tool that can be used to promote every point along the political spectrum. As sovereign countries, how can we carefully evaluate and use restraint so that as a global force, the Internet does not cause more harm than good?

2. TRANSFORMATION OF THE INTERNET

As countries attempt to control transborder information, the Internet is gradually transforming from an autonomous, unrestrained communication medium into a regulated and constrained one. Given the differences among countries, and the Internet's influence, a free and open Internet will not be acceptable to all political systems. While most countries, including the United States, Great Britain, and Germany are monitoring their Internet to detect political trends and public opinion (CITE) several countries, including India, China, Russia, Syria, Iran, and Saudi Arabia are actively censoring information (Levin, 2015; Rininsl, 2012). No countries are publicly acknowledging this shift, even those that continue to exert control of activities on their Internet. The scale and scope of such control varies across different countries, but the fact that most countries are exercising control needs to be consciously acknowledged. If the presence, nature, and reasons behind such control are unacknowledged, then the Internet will become simply a tool of the state, with no international or social oversight. I would argue that the sooner we consciously acknowledge this evolutionary change, and work towards open and balanced approaches, the better our chances will be of building a more constructive paradigm, and international norms, for the Internet.

We have seen controls being exerted on other fronts of the Internet already. As the economic security risks associated with the Internet have become more commonly known—from huge national and corporate cyber-breaches to the theft of an individual's identity—tremendous efforts have been expended globally to exert security and privacy controls. Politically and socially as well, some level of local control on the Internet may be necessary as we attempt to define and build consensus on a code of conduct that nations must follow to prevent deleterious social and criminal impacts.

An Approach to Sovereignty

Is a balanced approach to Internet sovereignty possible? We have seen the obvious advantages of a universal medium where people around the world can sustain global commerce, and interact with, and learn from, each other. The question is: Can countries allow such universal access and communication for citizens, while extricating content deemed harmful? The answer is, technically, yes, although, like many aspects of an open or Democratic society, it will be difficult. However, with a lot of searching, filtering, and legislation a balanced approach is possible. As traffic flows keep increasing, this balance may become more difficult; any fences created to filter Internet traffic will be both gigantic and porous, and difficult to manage effectively. It will be a constant struggle for governments to stay ahead of new censorship-evading techniques users will find to access and produce legally prohibited content. We have seen this already in cybersecurity, where there is a constant race to keep up with new hacking or cybercrime techniques.

For countries that want to impose stricter sovereignty, with complete censorship, the quest for the proverbial "forbidden fruit" will always push some users to evade censorship using proxies and other circumvention tools. While sovereignty and censorship are not synonymous, the motivation for several nation states in achieving Internet sovereignty will be to be able to censor Internet and social media to keep dissent under control. In a mobile international society with multiple forms of communication, it will be hard to keep citizens oblivious of contrary viewpoints. Inevitably those with vested interests and resources—which could in this context be cyber skills or the resources to hire them--will be able to access information, while people without such resources will be precluded.

One practical and viable option for countries with authoritarian governments that wish to censor the Internet might be to start with strong controls and then slowly open those controls enough to lessen the extreme difference in liberty their citizens will perceive with other countries, and to relieve pressures that could build towards revolution. Such gradual lifting of controls could permit a more controlled change towards freedom of expression that would eventually obviate the use of strong censorship.

The Internet cannot operate completely outside of the social and political mores of a country. It needs to be a reflection of society, rather than a disruptive force that can be used to destabilize political regimes or create societal harm. To understand the implications of a balanced approach to Internet sovereignty that provides some degree of control to individual nations, we discuss the alternate models of control, governance and ownership that have been used for such shared resources in the past.

3. MODELS FOR INTERNET OWNERSHIP: SOVEREIGNTY VS. COMMUNITY

There are two ways in which international resources are governed: 1) the concept of sovereignty; and 2) the concept of the Commons (Res Communis). The concept of sovereignty apportions territory to individual nation states, where a state has the right to control activities on its territory independently, and can enact local laws without interference from other states. States also have a duty to protect the interests of other states from (hostile) actions that originate within its borders. Res Communis maintains a resource as a collective to be shared by nation states, and the resource is governed through collective decision making, such as a treaty (Ku, 1990). For instance, the law of the seas has maintained the seas/oceans as a collective resource for all countries, partially because the sea cannot be governed like land resources, and the right to navigate the high seas is a universal law. Typically, governance of Res Communis resources is done through consensus building and International Treaties. Attempts at building such treaties to govern cyber resources have failed so far because of the irreconcilably different positions of different nations, and because those positions are often obscured by political posturing.

As an international resource, where does the Internet fall? Does it align with the sovereignty concept, or the concept of a shared collective? While the right to navigate the Internet is universal, the physical infrastructure (routers, cables, servers, etc.) of its operation lies within national borders, and is controllable by that nation. Except for the Internet address allocation and the global domain name system, the entire infrastructure is in local control. A key factor in determining if Sovereignty is the right model for the Internet is whether sovereign countries can effectively govern their Internet. Internet governance includes being able to provide the infrastructure, control access, and maintain Internet borders, which entails checking the credentials of each person (or packet) attempting to pass through the country gateway routers. From a conceptual point of view, since the physical infrastructure of the Internet is within country borders, it should be effectively controllable; the DNS and Internet address allocation can stay global without impacting a country's ability to control its internal resources. The challenge is that the border becomes a choke point, effectively shutting off the Internet from the rest of the world.

From a content point of view, as we have seen, countries are showing increasing ability to control the Internet. Even with ways of accessing banned content, laws and filtering provide enough impetus to tilt the debate in favor of sovereignty. Effective control of private communication is harder (and more contentious), especially since communication can be encrypted, and the identity of the communicators can be camouflaged. However, earlier arguments that states could not effectively govern and control the resource are slowly dissipating, as some states exert a great deal of control in terms of content, such as the Great Firewall of China (Dou, 2015) .

I believe that, since the Internet infrastructure today exists within national boundaries, and is subject to local laws, it lies within the national sovereign boundary of a country; however, the challenge will be to develop an internationally accepted set of norms that will allow multiple sovereign Internets to communicate with each other unfettered. With a more open international discourse about the advantages, rights and responsibilities of Internet sovereignty, we can address the fundamental problem that remains in implementing a more balanced sovereign concept, i.e. each country erecting borders around its own Internet.

A key difference between Internet borders and physical borders is anonymity. We do not let anyone cross geographical borders anonymously; they need to have passports to establish their identity and citizenship. While there would be free movement of Internet traffic within a nation, could there be an Internet passport (that reveals the identity of the user, and would be issued by a country to an individual) that would be required when traffic goes over a national sovereign Internet boundary? In other words, can states refuse entry of any data packets that do not carry the identity of the sender? If we increase the traceability of packets, especially those that originate from outside the country, we can start mitigating (not solving) several problems, including cross-border propaganda, international cyber crime, cyber warfare, and cyber espionage. This will not completely eliminate these problems, due to the ability of dissidents, foreign governments, and hacktivist groups to operate from within the country they are targeting, through volunteer recruitment and infiltration.

In my opinion, we need to move consciously towards a new paradigm of split or balanced sovereignty, whereby the Internet is divided into multiple segments, with some existing in a sovereign domain, and others in a shared or common domain. In order to chart an international path towards that new paradigm, we need to better understand its rights, responsibilities, and implications.

4. GLOBAL RESOURCE - GLOBAL RESPONSIBILITIES

With sovereign boundaries comes each country's responsibility to protect other countries' interests from hackers and criminals who operate within their own borders. International cyber crime today is committed with impunity across borders due to the reach of the Internet, and the anonymity of its users. Having a passport to accompany traffic that crosses an Internet border will make transborder Internet crime more traceable. Making it harder for criminals to camouflage their operations will deter malicious traffic. Also, once an international process is established to prosecute such crimes, attribution would become more reliable.

Such traceability may also limit patriotic hacking, where citizens of one country directly launch attacks against the citizens or government of another country. Through these attacks, citizens feel empowered; they can act instead of silently suffering perceived injustices. Governments have tacitly supported such activities for political and strategic reasons. However, this powder keg can explode at any time; citizen hacking armies can turn against their own governments very quickly. There are ways around censorship and control of the Internet, and if a large number of people are determined, Internet controls become very difficult to implement, as in the Middle East revolutions, where social media was used to mobilize citizen actions and broadcast what was happening in real time.

Will there be a place for civil disobedience and protest if greater Internet sovereignty existed? Would countries in North Africa and the Middle East have been able to avoid the instability and revolutions that have pushed them towards chaos? The key to this is the role of international actors as destabilizing factors. Outside influence definitely played a part in instigating unrest during the Arab Spring, but a large part of the instigation was agents working on the ground to organize internal forces. I do not believe having a controlled Internet border would have prevented the Arab Spring revolutions, neither will it prevent citizen-led revolutions in the future. Ultimately, the Internet and social media are simply tools; in and of themselves they can neither cause revolutions nor effectively quell them. Social media allows protestors and revolutionary groups to lower the costs of organizing, and to broadcast messages quickly and widely; after all, a single Facebook post or Twitter feed can reach hundreds of thousands of people in an instant. However, that audience must be receptive and ready for action, not simply to "like" the political sentiments. Social media and Internet also have their limitations; posts can be tracked, and turned into State tools to collect intelligence, prosecute protesters, and spread disinformation. Posts, profiles and networks can be mined effectively for counterintelligence and prosecutorial networks. The State can also shut down movement websites, as we see regularly in Iran and China during times of social unrest. (Papic, Noonan, 2011)

After the Internet shutdown in Eqypt in the end of January, 2011, protestors used pamphlets, faxes, landlines and the Speak to Tweet service to get their message out. Within these Arab Spring protests we can clearly see both the power and limitations of these tools, whether used by protestors or the State. As a mass communication medium, the Internet will continue to provide citizens with a venue for debating and organizing. But protests will still depend—ultimately--on the ability to rally people to action, and to use multiple strategies, especially in countries where communication is controlled. States will not be able to effectively shut down the Internet, yet they can mine it effectively to counter unrest. It may indeed be that the Internet, as it continues to evolve, will act as a deterrent to oppressive political forces, making it more difficult for such hardened autocracies like Iran and Myanmar to sustain their regimes. However, that will depend on the will of the people; the Internet and social media are tools, and not political forces in themselves. In a balanced sovereignty model, countries must, in exerting controls, make sure that they preserve the freedom of expression that they advocate for, based on the culture and norms of their people.

What might be the operational impacts of increasing Internet border controls? These could be tremendous, with massive delays associated with the processing of information, coordination of identities, and filtering through-traffic. Clearly, such problems will only increase as the traffic does. There will still be people who are able to spoof their identity, rendering their 'Internet passports' meaningless. Even with the creation of a global identity system there will be transgressions; and countries will still engage in subterfuge to get their agents access to other countries for transborder espionage, propaganda, and attacks.

The societal impact of Internet Sovereignty is quite unpredictable. Would Internet borders dissuade communication between people of different countries, limiting the content of the Internet to nation states? Will we regress to a divided world on the Internet? Would there be new limits, restrictions and embargos, to International Trade? These are all possible, unpredictable outcomes of moving from a common to a divided resource. Some of the answers will depend on the effectiveness of the controls, and the ongoing commitment to freedom of expression that countries exert on their Internet.

Given the differences in culture, society, and forms of government among countries, and the Internet's influence in shaping them, a completely free and open Internet will not be acceptable to countries that feel that their cultural values, and even their political systems could be threatened. Clearly, the time has come for the creation of a new paradigm of split sovereignty of the Internet, where states have some control of content inside their borders based on their society's culture, laws, and expectations. Since this is an evolutionary change that was bound to, and is happening, it needs to be acknowledged and consciously addressed. The technical means are available, and new means can be developed through mutual dialogue, to bring more traceability, transparency and responsibility to the Internet. But is this new paradigm of split or balanced Internet sovereignty--with some segments existing in a sovereign domain, and others in a shared or common domain—feasible? And if so, what might the impacts be? I would like to address these important issues of feasibility and implications next.

5. FEASIBILITY AND IMPACT

Will it be technically possible to achieve a balanced, or split sovereignty of the Internet? As cybersecurity experts, analysts and technicians, there are many practical questions to address in order to predict, prepare for, and navigate this evolutionary change, including: 1) Sovereign operational control. The delineation of sovereign Internet borders, and implementation of controls that reflect a country's legal and social expectations, especially in relation to freedom of speech and privacy; 2) International Rules and Responsibilities. The definition of, and building of consensus around, international rules of conduct on the Internet, and the creation of a forum for dispute resolution; 3) Securing the Critical Infrastructure. Expanding the paradigm of balanced sovereignty to the Internet of Things; and 4) Social Media & Communication on the Internet. Limitations that reflect mutual freedom of expression and privacy values.

5.1 Sovereign Operational Control of the Internet:

The protocols for the Internet are standard, and the equipment is built on those standards. No matter how the Internet is governed, the fundamental universality of the infrastructure will not change. The main point of contention in governance remains the distribution of domain names, and the control of the Domain Name Servers. No matter what decisions are made on governance, short of countries separating themselves from the global Internet, the universality of Internet operations will not be impacted.

Yet, Operation of the Internet is not a purely technical issue. Sovereignty on the level of Operational control also involves the laws that will ensure that such control reflects the freedom of speech and privacy mores, ideals, and expectations of the country and its citizens. As has been effectively demonstrated by several countries, control of content is feasible through a combination of filtering, content laws, and monitoring. What needs to be part of the conversation, and the evolution of the Internet, is that such sovereign control, as a function and reflection of the laws and mores of a country, cannot be simply a tool of the State, but must also extend to, and govern a country's government agencies as well as its citizens.

Countries also have different ideals and expectations in relation to privacy, which need to be considered, and reflected in any sovereign control of the Internet. Russian, Chinese, and

American citizens may hold different expectations about their rights to privacy in communicating with other citizens in their country. Again, the monitoring and control of content has proven to be feasible, but aligning that control with a country's social expectations and legal precedents in relation to privacy and freedom of expression will be an essential aspect of this evolution.

5.2 International Rules and Responsibilities

The Internet has become a key propaganda tool, whereby: 1) countries are leveraging it to spread propaganda and hacktivist attacks against countries where they have conflict; 2) terrorist organizations use it to spread their messages and recruit conscripts; and 3) hackers and criminals flood it with malware. A key aspect of the evolution towards a new paradigm of split or balanced sovereignty will be building international consensus around rules and responsibilities of Internet conduct.

Is there international consensus for what constitutes criminal acts, and acts of terrorism, on the Internet? And if countries want to exert more control to protect their citizens from such acts, are they willing to accept responsibility for acts committed by their own citizens against other sovereign nations? This is a key challenge; currently anonymity and misdirection are used very effectively to prevent identification of perpetrators and attribution of crimes; there is no universal mechanism for identifying Internet threats, for tracing attacks back to the perpetrators, or for prosecuting those criminals. The cyber crime treaty proposed in Budapest two decades ago meant to provide mechanisms for tracking international cyber criminals is still in limbo, with several contentious issues, including: 1) unfettered access across borders 2) traceability 3) access of data from ISPs to identify perpetrators 4) time sensitivity of the mechanism 5) sharing of data among countries and validating the data received. Political will must supersede suspicions and distrust among nations to build such consensus.

5.3 Securing Critical Internet-based Infrastructure

How can this new paradigm of split, or balanced Internet sovereignty be expanded as societies develop more complex networks of physical objects, devices, vehicles, and buildings embedded with sensors, and network connectivity, the Internet of Things? Power and transportation are increasingly dependent on the use of ICT technology, though we should distinguish between Internet connectivity and the use of ICT for communication networks. Both the Power Grid and the Transportation network are moving towards the SmartGrid and connected vehicles; they will rely heavily on universal communication networks for improved efficiency, new functionality, and resilience. However, that does not mean that they are connected to a completely shared, global Internet; they will have their own network within sovereign boundaries, and countries will be free to define security and traceability on their networks as they see fit.

There is also a fundamental difference in power and transportation; whereas the power grid relies on a single monolithic network, the traffic grid will be millions of ad hoc networks that communicate with each other in local neighborhoods. While power and transportation will have very different threats that need to be understood, both domains will need to define connectivity in the infrastructure at sovereign boundaries. It is not just the digital networks that cross borders, but also the physical infrastructure---power lines and roads; how can these be secured under the split/balanced paradigm? Banking and Internet infrastructure are even trickier to manage under rules of sovereignty since they both require global connectivity and must follow international standards and norms. These will have to be managed more carefully in a sovereign Internet regime, such that they retain their universality while adhering to globally acceptable norms and standards.

5.4 Social Media and Communication

Social media will also be difficult to manage in a sovereign Internet regime without restricting peoples' choices. Preventing people from communicating and building relations with people in other countries would be a mistake. It would perpetrate the gravest limitations of nationalism, promoting feelings of distrust and misplaced jingoism among citizens, and lead people to find ways to circumvent controls. We have gone too far to completely pull back on communication among citizens across borders; monitoring the Internet with limited restrictions on the content will perhaps be the direction that most democratic (vs. autocratic) countries will go.

Conclusions

The Internet has given society a great opportunity to create a more unified world where cultural norms and values can be shared and harmonized. It has given voice to the oppressed, provided a window into inaccessible regions of the world, given access to small businesses, entertainment to the poor, and markets to otherwise marginalized players. On the other hand, it has provided universal access to pornography, allowed terrorists to recruit new members, unleashed revolutions, and allowed unprecedented access for criminals to commit crimes. Given its reach and power, its governance has become a source of contention among nations with differing political views and cultural norms. Based on their cultural and social norms, countries are increasingly trying to exercise sovereignty on the Internet within their borders. The pros and cons of such sovereign control can be debated, as we have done today; however, based on technological developments and growing unease among nations, some level of Internet sovereignty is inevitable. We need to work towards a new paradigm of balanced sovereignty whereby global connectivity is not completely subjugated to the whims of individual nations, while nations are allowed some ability to exert protective controls that reflect their shared values of freedom of expression. The only path towards such evolutionary growth for the Internet is a conscious and open one, through international dialogue.

REFERENCES

Brown, I., and Kroff, D. (2015) Terrorism and the Proportionality of Internet Surveillance, European Union responses to terrorist use of the Internet *Cooperation and Conflict June 1, 2015 50: 250-268*

1) Dou, E. (2015, January 30). China's Great Firewall Gets Taller. *Wall Street Journal.* Retrieved from http://www.wsj.com/articles/chinas-great-firewall-gets-taller-1422607143

2) Fielding, N., & Cobain, I. (2011, March 17). Revealed: US spy operation that manipulates social media. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

3) Ku, C. (1990). The concept of res communis in international law. *History of European Ideas*, *12*(4), 459–477. http://doi.org/10.1016/0191-6599(90)90002-V

4) Levin, D. (2015, December 16). At U.N., China Tries to Influence Fight Over Internet Control. *The New York Times*. Retrieved from http://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html

5) Papic, M., & Noonan, S. (2011). Social media as a tool for protest. *Stratfor Global Intelligence*, *3*.

6) Rininsl, A. (2012, April 16). Internet censorship listed: how does each country compare? *The Guardian*. Retrieved from http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list