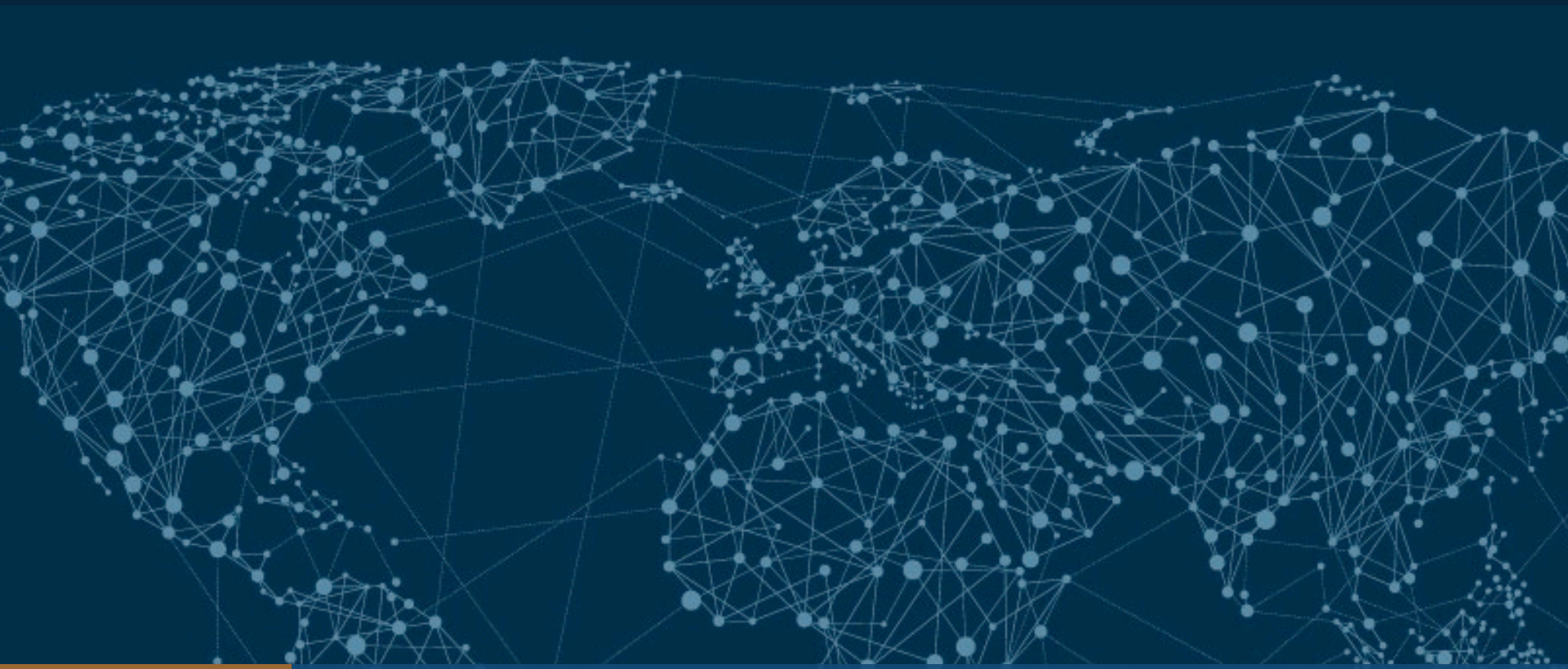

At-Large Capacity Building WG, 3d Webinar of the At-Large Capacity Building Program 2020 on “Geopolitics and Cybersecurity”

Multistakeholderism, Cyberfreedom and End-Users

Javier Rúa-Jovet, ALAC

June 1st, 2020

Introduction

The Internet was born amidst geopolitical tensions, and still faces them. Although conceived for the military purposes of a superpower, a communications system capable of resisting a nuclear attack, its gestation and development - the construction of its protocols and rules - is the product of the consensus and collaborations between a community of university-based, non-governmental engineers; a constant, progressively inclusive and open construction process that continues today.

Even though these processes have been clearly successful, many states persistently reject this free, open, generally private governance model, as it breaks with traditional, state-centered international-law policy making.

Introduction

The global Internet, as any market, cannot be truly free or fair without legal parameters. The establishment of norms for the prevention and prosecution of international cybercrime, while keeping the Internet open and free is such a normative endeavor.

Humanity faces two critical options to successfully address any global challenge, be it viral pandemics, governance of the Internet or balancing cybersecurity with cyberfreedom.

The first is between totalitarian vigilance and human empowerment. The second is between nationalist isolation and global human solidarity.

Introduction

Simply put, effective, free, trust-based global cooperation is essential to effectively and reasonably address cross-border issues, be they pandemics, nuclear proliferation, climate change, or cybersecurity.

How can we best achieve effective, free, trust-based, cooperative global norm-making to effectively address international cybersecurity issues, while also keeping the Internet free?

Is Multilateralism the only way?

Multilateralism vs. Multistakeholderism

Traditional "International law" lawmaking is either bilateral or multilateral. In both cases its intergovernmental: sovereign states talk to sovereign states and make legal decisions. These decisions take the form of law binding on these states via treaties and/or via universal consistent legal state practice. (*see*, Statute of International Court of Justice, Art. 38, https://www.icj-cij.org/en/statute#CHAPTER_II)

Multistakeholderism promotes the participation of all interested private & public actors. By involving everyone in an open, transparent and collaborative discussion, the decisions achieve great trust & acceptance from the various private & public parties with interest. It treats private persons, & groupings of persons (both natural & juridical) as equal stakeholders to governments.

Would a multistakeholder approach in international cybersecurity discussions provide better outcomes? Is there even a path for non-governmental stakeholders to impact these processes?

A path for end-user's input at cybersecurity policymaking?

There does not seem to be a path for Internet end-user, or groupings of end-users, to impact outcomes in processes/bodies such as GGE & OEWG.

An open UN avenue for dialogue is the Internet Governance Forum, the formal platform under UN auspices for governments, companies, technical experts, and civil society to engage on internet and technology policy. (https://www.intgovforum.org/multilingual/tags/about)

The UN Secretary-General recently made statements, in the context of IGF-XI, Berlin (2019), which point towards an opening for non-state voices to inform Cybersecurity/Cyberfreedom discussions.

(find at: https://www.un.org/sg/en/content/sg/speeches/2019-11-26/remarks-internet-governance-forum)

A path for end-user's input at cybersecurity policymaking?

Inter alia, the Secretary General expressed:

"Artificial Intelligence applications can be used to monitor and manipulate behaviour, to besiege us with ever more targeted and intrusive advertising, to manipulate voters, to track human rights defenders and to stifle expressions of dissent.

How do we safeguard privacy in an age of artificial intelligence, facial recognition, location monitoring, biometric sensors and the Internet of things?

How can we ensure that human rights obligations apply online as they do offline?
The Office of the High Commissioner on Human Rights and others are working on the urgent task of understanding better how exactly international human rights can be applied in cyberspace. […]

You are also aware of the growing efforts of some States to construct ever harder borders in cyberspace, on the one hand, and the ever-increasing number of cross-border cyber-attacks, on the other.

[Continues]

A path for end-user's input at cybersecurity policymaking?

[Continued]

Low-intensity cyber-conflict between major States is not a future prediction but a feature of our present time. In such a climate, mechanisms that build trust and cooperation are indispensable.

The growing frequency and severity of cyber-attacks are undermining trust and encouraging States to adopt offensive postures for the hostile use of cyberspace. […]
Allow me to propose three ways in which this Internet Governance Forum can lead the way.

First, let us build this Forum into a platform where government representatives from all parts of the world – **along with companies, technical experts and civil society – can come together to share policy expertise, debate emerging technology issues, agree on some basic common principles, and take these ideas back to appropriate norm-setting fora.** […]

Lastly, I will soon appoint a Technology Envoy to work with governments, industry and civil society to help advance international frameworks, and nurture a shared digital future that puts people first and helps bridge the social divide. […]"

The *People of the Internet* and Multilateral Walls

'*We the People of the Internet*', must find ways to defy or circumvent multilateralism's barriers to entry.

All individual or joint, non-governmental Internet stakeholders, must somehow claim our independent and equal voice and seat at all possible "cyber-tables" alongside states, not under states, (something that has already fully happened in the limited ICANN DNS/IP space.)

ALAC, as the 'primary organizational home" within ICANN for the interests of Internet end-users, could be an appropriate place to discuss some of these plans and attempt to formulate joint community postures.

Substantial challenges in “Internet-people building”

We all appreciate the decision making challenge in ALAC, given the great diversity of backgrounds, viewpoints and ideologies present.

Also, the margin for creative joint ALAC advocacy, for example in cybersecurity/cyberfreedom matters, is further restricted given that action must connect to ICANN’s very limited remit: the technical coordination of the Internet's domain name and addressing system.

Also, the process of creating an effective “Internet People”; a generally autonomous transnational civil community capable of credibly and coherently challenging and standing against *Westphalian** worldviews, structures and institutions, requires critical, very difficult political alliances between private sector entities as a precondition, to achieve the necessary firepower for the task.

(*The ‘Peace of Westphalia of 1648’ is the series of treaties that ended the state of persistent warfare in Europe after the Protestant Reformation of 1517. It marks the birth of the new European order based on the concept of national sovereignty, mutual recognition between sovereigns and non-interference.)

Substantial challenges in “Internet-people building”

In the words of Milton Mueller, this task requires:

> “[…] [a]n alliance between multinational businesses seeking trust and accountability across a global marketplace and transnational civil society actors motivated by concerns about privacy and civil liberties. Only a business-civil society alliance can prevent a dangerous alliance between state intelligence and law enforcement agencies and the major private sector intermediaries who control much of the data.” On transnational popular sovereignty, (Mueller, WILL THE INTERNET FRAGMENT?, Polity Press, 2017, p. 147:

But are we up to the task?

Identifying the pertinent cyberfreedoms is the easy part

Individuals & groupings of individuals can, in available International fora, stand in opposition to authoritarian states, and could even state better defenses than liberal states in regards interests/rights such as these:

-Guarantee that Interception of communications, collection, analysis and use of data over the Internet by law enforcement agencies should be for purposes that are specifically authorized by international human rights treaties and enabling local statutes.

-Control of State restrictions of message encryption technologies.

-Right of Internet end users to not be subjected to technical DNS abuse; for example, a right to be free from unconsented malicious software, like viruses, spyware, ransomware, spyware, regardless of private or public origin.

-There are surely many others and *You*, The People of the Internet, can and should come up with many more and fight for their recognition in all pertinent policy or law making contexts !

Ideas?

Epilogue: The Elephant in the (Post-Covid) Room

More questions than answers:

Will the post-Covid world strengthen nation-states & strengthen nationalisms? Will state-centered governance models be preferred henceforth locally & globally? Are we condemned to a less open, less prosperous & less free 21st century; a century of control? Will Cybersecurity trump Cyberfreedom & human rights?

The battle over a free Cyberspace; for the liberal essence of the Internet; for the rightful place & rights of private individuals & groupings of individuals in its governance, might be more crucial than ever in post-coronavirus world. A world where imposition of state sovereign power seem progressively unquestioned & accepted; where fear –the opposite of trust- begets autocrats & autocrats beget more fear.

Or, could a new internationalism be forged; a new global system, with new forms of social security & systems to manage human interdependence & well-being? Will the current crisis give the necessary push for public & private liberal democratic leadership to wake up, improved, with more rational, & more effective local & global governance institutions? Or better yet, could we eventually see a strengthening of multistakeholder approaches & transnational institutions, opening new international spaces for individual & collective non-state voices? The jury is still out.

Thank you