EGMONT

The emergence of cyber diplomacy in an increasingly post-liberal cyberspace

By Andre Barrinha, (https://www.egmontinstitute.be/expert-author/andre-barrinha/) Thomas Renard (https://www.egmontinstitute.be/expert-author/thomas-renard/) (11 June 2020)
In Commentaries (https://www.egmontinstitute.be/publication_parent/commentaries/)

EU and strategic partners (https://www.egmontinstitute.be/core/eu-and-strategic-partners/), EU strategy and foreign policy (https://www.egmontinstitute.be/core/eu-strategy-and-foreign-policy/), European defence / NATO (https://www.egmontinstitute.be/core/european-defence-nato/)

Behind some recent discussions on internet governance, there is a broader contest for power and values in cyberspace. This contest is a sign of the so-called "post-liberal order". As a result, cyber-diplomacy becomes ever more needed to avoid a full fragmentation of cyberspace.

This article was published in Net Politics*, a blog of the Council on Foreign Relations (CFR), on 10 June 2020.*

(Photo credit: piqsel.com)

*****

The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace

In September 2019, a Huawei led-group (https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2) that included China Mobile, China Unicom, and the Chinese Ministry of Industry and Information Technology proposed a significant overhaul of the internet: A new top-down internet protocol called "New IP (https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAAE74dv2OvZLUV4NA7s1qauTyZOX1KFIF2vGPOa0AlzDQKMFApwoaWuv6dsfftI0kBoFV03CHP_kKV92cmb901dSF5cyb0GP0GnZUL1OQFFJGQX6uzT-rwy38DuesxBys19cA76s3c5Y5NCdJiuDg4pj-vaLpGN0SOMOffBH0n4f9)." In their view, the proposed New IP would better support (https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/) the coming ultra-interconnectedness of the physical and digital worlds through virtual reality, driverless cars, internet of things (IoT) and other emerging technologies. The group also argued that the internet in its current form has "lots of security, reliability and configuration problems (https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf)" [PDF]. Beyond these technical considerations, some read this proposal (https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f?shareType=nongift) as another chapter in a broader political move, which China and some other countries have been conveying for a while (https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/UN-110912-CodeOfConduct_0-1.pdf) [PDF]: cyberspace can no longer be dominated by the West and needs to reflect the new balance of power in the international system.

This echoes an argument that we developed in "*Power and Diplomacy in the Post-Liberal Cyberspace* (https://academic.oup.com/ia/advance-article-abstract/doi/10.1093/ia/iiz274/5722299?redirectedFrom=fulltext)." The liberal international order, we argue, was articulated mainly around three concepts: Western power, liberal values, and Western-dominated institutions. As we venture towards the end of the first quarter of the twenty-first century, international relations are becoming increasingly "post-liberal (https://academic.oup.com/ia/article/94/1/25/4762688)." Although the exact contours of the new order are still in the making, it will certainly be less Western, less liberal and potentially less cooperative.

Cyberspace is also becoming increasingly post-liberal. The power relations, values, and institutions that governed it since its initial development in the 1960s are being challenged by those that did not have a say in how it was structured. Although international divergences over internet regulation can be traced back to the 1990s, they are now more intense than ever.

The New IP proposed by the Huawei-led group can be seen as part of a broader, albeit not necessarily interconnected set of initiatives that aim to rebalance power relations in the regulation of cyberspace. Some of these initiatives have been introduced in the United Nations, where the global cybersecurity agenda was originally driven by discussions held by the Group of Governmental Experts (GGE). In September 2018, the UN General Assembly approved the creation of not one, but two parallel processes (https://dig.watch/processes/un-gge) for the first time. One was the U.S.-sponsored sixth edition of the GGE. The other was the Open-Ended Working Group (https://www.cfr.org/blog/first-global-meeting-cyber-norms) (OEWG), proposed by Russia and open to all UN member states. These two processes have partially overlapping membership (all the GGE members are also, by default, OEWG members) and discuss very similar issues during (roughly) the same period. The 109 votes in favor of Russia's proposal to form the OEWG clearly signaled many governments' support for a broader discussion beyond the exclusive GGE and new perspectives on cybersecurity and internet governance that differ from those championed by the West for decades.

Last year, Russia also proposed (https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet) the creation of another committee of experts with the ultimate aim of developing an international cybercrime treaty to replace the Council of Europe's Budapest Convention (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185). Russia's resolution was approved (https://www.undocs.org/A/74/401) [PDF] by seventy-nine states—including swing states such as India,

Indonesia and South Africa—with thirty-three abstentions, while sixty states voted against it. This revealed, once again, the attractiveness of not only Russian initiatives, but also new non-Western efforts to determine how cyberspace is governed internationally.

The New IP proposal further highlights the role played by big tech in shaping the geopolitical debate on cyberspace. Discussions on the geostrategic and security implications of a 5G infrastructure dominated by Huawei ruled the pre-COVID-19 agenda and have even been included in multiple conspiracy theories (https://www.wired.co.uk/article/5g-coronavirus-conspiracy-theory) on the topic. In the West, Microsoft (https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace), Siemens (https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity/cybersecurity-charter-of-trust.html), and other companies are also actively contributing to the debate on responsible state behavior, often exhibiting state-like behavior themselves. For example, Microsoft recently announced the creation of its UN representation office (https://blogs.microsoft.com/eupolicy/2020/01/17/senior-gov-affairs-leaders-appointed-brussels-new-york/) that, among other aims, will "focus on advancing Microsoft's partnerships with the United Nations and its agencies."

The Emergence of Cyber Diplomacy

While the liberal international order enabled the development of cyberspace, the move towards a post-liberal order has seen the advent of cyber diplomacy (https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924), i.e., the use of diplomatic resources and the performance of diplomatic functions to secure national interests in cyberspace. In the last decade, dozens of foreign ministries have been creating offices exclusively dedicated to cyberspace and appointing "cyber diplomats (https://www.eastwest.ngo/interactive/timo-koster-cyber-diplomacy)" in order to respond to the growing politicization of cyberspace and broader techno-geopolitical dynamics. This move has concentrated more international cyber policy activities in foreign affairs ministries, elevating the issue in government hierarchies and increasing the level of international activity of each state in cyberspace.

In a world in which more countries are acquiring offensive cyber capabilities (https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities), cyber diplomacy is needed to prevent escalation or wrongful attribution of cyberattacks by maintaining a constant dialogue between peers and ensuring channels of communication remain open, even in times of crisis. It also is necessary for developing binding and non-binding norms of responsible state behavior in cyberspace and addressing the most acute divergences between stakeholders in this area. This is possible through multilateral fora such as the GGE and the OEWG, regional efforts like the Organization for Security and Cooperation in Europe (OSCE) (https://www.osce.org/pc/227281?download=true) [PDF] confidence-building measures, and bilateral agreements such as the 2015 U.S.-China Cyber Agreement (https://www.cfr.org/blog/top-five-cyber-policy-developments-2015-united-states-china-cyber-agreement).

Overall, in a cyberspace that used to be predominantly regulated by IT experts and engineers, cyber diplomats are now actively navigating between trying to generate consensus among stakeholders and, as a last resort, building bridges between fundamentally different, if not incompatible visions. The former demands an acceptance of the lowest common denominator, possibly sacrificing core values in the name of a stable international order of cyberspace. The latter entails a recognition of the failure to maintain a homogeneous cyberspace and the acceptance of less interconnected networks (https://www.chathamhouse.org/expert/comment/tackle-splinternet). As conflicting visions for the future of the global internet inevitably collide, cyber diplomats will have to negotiate these difficult choices.

Andre Barrinha is a senior lecturer in international relations at the University of Bath, UK.

Thomas Renard is a senior research fellow at the Egmont Institute, Belgium.

EGMONT

Royal Institute for International Relations
Rue des Petits Carmes 24A
1000 Brussels - BELGIUM

POSTAL ADDRESS

Rue des Petits Carmes 15
1000 Brussels - BELGIUM

CONTACT

+32 (0)2 223 41 14
info@egmontinstitute.be (mailto:info@egmontinstitute.be)