Accepted Manuscript – Published in *International Affairs* (OUP)

Power and diplomacy in the post-liberal cyberspace

ANDRE BARRINHA AND THOMAS RENARD

It is becoming increasingly consensual that we have or are now transitioning from an international liberal order to a different reality. Whether that reality is different solely in terms of power dynamics, or also in terms of values and institutions is up for discussion. The growing body of literature on 'post-liberalism' is used as an entry-point for this article, which aims to explore how the post-liberal transition applies to cyberspace. We explore how power dynamics are evolving in cyberspace, as well as how established norms, values and institutions are contested. This article then looks at the emergence of cyber diplomacy as a consequence and response to the post-liberal transition. As it will be argued, if cyberspace was a creation of the liberal order, cyber-diplomacy is a post-liberal world practice. What role it plays in shaping a new order or building bridges between different political visions, and what it means in terms of the future of cyberspace, will constitute key points of discussion.

In 1996, in reaction to the growing online presence of governments and private actors, the libertarian John Perry Barlow wrote his Declaration of the Independence of Cyberspace. 'Governments of the Industrial World,' where he said, 'You are not welcome among us. You have no sovereignty where we gather.'[1] Power politics and business interests were resisted by those nostalgic for the space of freedom and exchange that was the internet of the early days, free and open to anyone with access to a computer.[2] More than 20 years later, the old libertarian ideal sounds even more utopian. 'Geopolitics is back' in the physical world,[3] and it is creeping

[1] John Perry Barlow, 'A Declaration of the Independence of Cyberspace', Electronic Frontier Foundation, https://www.eff.org/cyberspace-independence. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 27 Nov. 2019.)

[2] Milton L. Mueller, *Networks and states: the global politics of internet governance* (London: MIT Press, 2010), pp.2-3.**{?}**

[3] Walter Russel Mead, 'The return of geopolitics: the revenge of the revisionist powers', *Foreign Affairs* 93: 3, May–June 2014, pp. 69-79.**{?}** https://www.foreignaffairs.com/articles/china/2014-04-17/return-geopolitics.

into cyberspace, which has become a ‘new arena for competition among states’[4]—a competition about values and interests, norms and ideas.

This article seeks to link these discussions and concerns to the broader literature on the post-liberal order. It explores how the demise of the liberal order affects cyberspace. More fundamentally, it focuses on the consequences of a post-liberal cyberspace for the global order, with a focus on the concept of ‘cyber diplomacy’,[5] which entails ‘the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace’.[6] In our view, whereas cyberspace was a creation of the liberal order, cyber diplomacy is eminently post-liberal: its existence results from the acknowledgement that cyberspace is a contested arena in which traditional diplomatic skills need to be employed in order to prevent conflict and generate stability.

The ‘liberal order’ era that emerged after the end of the Second World War created the necessary conditions for the development of computer networks, initially limited to the United States, but rapidly expanding across Europe and other parts of the world. These conditions included a combination of immense state investment in science and technology during the Cold War with excellent research facilities and an underlying ideology that rewarded creativity and innovation. For instance, the Pentagon-sponsored ARPANET—the ancestor of the internet—was created in 1969, linking four US universities (the University of California at Los Angeles, Stanford, Santa Barbara and Utah). Ray Tomlinson, the inventor of the email, was working for an American company (BBN Technologies), and Tim Berners-Lee, a researcher at the European CERN in Switzerland, was responsible for the development of the HyperText Transfer Protocol (HTTP) that enabled the creation of the World Wide Web.

With the end of the Cold War, the protocols and institutions developed in the West consolidated this new space of social, political and economic activity globally, facilitated by an extensive physical infrastructure. Cyberspace was not only a creation of the liberal order, but was deeply infused by its values and principles, and played an important role in globalizing them: it opened

[4] Michèle Flournoy and Michael Sulmeyer, ‘Battlefield internet: a plan for securing cyberspace’, *Foreign Affairs* 97: 5, Sept.–Oct. 2018, pp. 40–46.

[5] Whereas digital diplomacy is usually seen as ‘the application of digital tools to diplomacy’, cyber diplomacy refers to ‘the application of diplomacy to cyberspace’. See Shaun Riordan, *Cyberdiplomacy: managing security and governance online* (Cambridge: Polity, 2019), p. 5.

[6] André Barrinha and Thomas Renard, ‘Cyber-diplomacy: the making of an international society in the digital age’, *Global Affairs* 3: 4–5, Feb. 2017, pp. 353–64.

the way for the digitalization of the global economy and the global networking of citizens worldwide. The internet, in particular, was the definitive technology to make the world a 'global village'.[7]

Progressively, however, the configuration of cyberspace evolved. The balance of technological innovation tipped away from the public sector to the private,[8] with major companies such as AOL, GeoCities and Altavista in the late 1980s and early 1990s and later Google, Amazon, Facebook and Apple dominating how we interact with the Web. Internationally, internet governance developed predominantly according to a multistakeholder model, in which companies, NGOs and other actors sat side by side with government agencies and international organizations. Organizations such as the Internet Engineering Task Force, which played (and still plays) a central role in keeping the internet running, followed 'the web's early ethos', with a highly decentralized and informal approach to decision-making.[9] Cyberspace was enabled by and further enhanced the West's technological hegemony. But while these companies were all 'western', this bias was changing too, as non-western governments and companies entered the game.[10]

To this day, one can argue, the internet remains at least partly western-dominated: although most internet traffic is now generated outside the West, the internet root servers are still mainly based in the United States.[11] However, it is widely agreed that we have made, or are now

[7] Marshall McLuhan, *Understanding media* (Boston: MIT Press, 1964).

[8] Peter W. Singer and Allan Friedman, *Cybersecurity and cyberwar: what everyone needs to know* (Oxford: Oxford University Press, 2014), p. 14; Madeline Carr, *US power and the internet in international relations: the irony of the information age* (Basingstoke: Palgrave Macmillan, 2016).

[9] Adam Segal, *The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age* (New York: PublicAffairs, 2016), p. 208.

[10] Carr, *US power and the internet in international relations*, p. 129.

[11] This sense of western superiority in cyberspace is highly salient in Russia's political narrative, with crucial consequences in terms of how Moscow engages with information security. In 2014, Dmitrii Peskov—the Kremlin's spokesperson—called the US 'the global internet's main administrator'; more recently, in 2018, Vladimir Putin told American journalist Megyn Kelly that 'the internet is yours [the United States']'. See Lincoln Pigman, 'Russia's vision of cyberspace: a danger to regime security, public safety, and societal norms and cohesion', *Journal of Cyber Policy* 4: 1, 2019, p. 25.

making, the transition from an international liberal order to a different reality.[12] This new reality is clearly mirrored in cyberspace, as we will argue in this article, and cyber diplomacy plays a central role in negotiating its distinct power balances, values and institutional changes.

Cyber diplomacy is a recent practice in international relations. Although the emergence of international contention in the cyber domain,[13] particularly regarding internet regulation, goes back to the 1990s,[14] only in the past decade have states started to understand (and act on) the full geopolitical impact of the widespread use of computer networks. The interconnectivity of modern life was no longer an issue merely for IT specialists and engineers, but also for the traditional diplomatic apparatus. As we argue, the rise of cyber diplomacy coincides with a growing contestation of the values, institutions and power dynamics of the liberal-created cyberspace. In consequence, cyber diplomacy is a practice that is always shifting between bridge-building dynamics and the defence of long-held national (and regional) principles and interests: a difficult balance to achieve, in an area where stakes are constantly rising. After all, what happens in cyberspace is very much at the core of the politics, society and economics of the twenty-first century.

This article will start by contextualizing the discussion on the post-liberal order, focusing on the dimensions of power, values and institutions, followed by its application to cyberspace. It will then explain how cyber diplomacy can contribute to addressing some of the challenges of post-liberal cyberspace. The article will conclude with a reference to some potential scenarios for the post-liberal order transition in cyberspace and the role of cyber diplomacy therein.

[12] G. John Ikenberry, ‘The end of liberal international order?’, *International Affairs* 94: 1, Jan. 2018, pp. 7–24; Wu Xinbo, ‘China in search of a liberal partnership world order’, *International Affairs* 94: 5, Sept. 2018, pp. 995–1018; Joseph S. Nye Jr, ‘The rise and fall of American hegemony from Wilson to Trump’, *International Affairs* 95: 1, Jan. 2019, pp. 63–80; Peter Trubowitz and Peter Harris, ‘The end of the American century? Slow erosion of the domestic sources of usable power’, *International Affairs* 95: 3, May 2019, pp. 619–40.

[13] See Marianne Franklin, *Digital dilemmas: power, resistance, and the internet* (Oxford: Oxford University Press, 2013).

[14] George Christou and Seamus Simpson. ‘Gaining a stake in global internet governance: the EU, ICANN and strategic norm manipulation’, *European Journal of Communication* 22: 2, 2007, pp. 147–64.

Framing the post-liberal challenge

It is commonly accepted that the scope of the liberal order varied across time, space and domain.[15] This system was neither universally liberal, nor always 'ordered', as attested by the multiple moments of conflict during the Cold War, and the explosion of identity wars in the 1990s.[16] Nor was it truly universal, as US hegemony only realized itself at the end of the Cold War, and even then the 'unipolar moment' had its limits. As several scholars have emphasized, there have been multiple layers of 'order' during the past decades—regional and subregional orders, competing or overlapping with macro-orders, such as the 'liberal order' and the 'Cold War balance of power'.[17]

The liberal order evolved under US leadership in the post-Second World War era, based on a set of norms (international law) and values (such as free trade, democracy and human rights), progressively promoted through and empowered by a **{1}** multilateral system. There are multiple academic and policy debates on how we are now moving away from that order, towards a post-liberal context. Some of these debates focus on the issue of power shifts, with rising powers challenging the US hegemony in the economic realm first, but also increasingly militarily and diplomatically. Authors diverge in their assessments, but tend to agree 'that the hegemony of the liberal world order is over'.[18] In this sense, 'post-liberal' essentially means 'post-western',[19] or 'post-American'.[20] The term is also associated with a 'crisis of authority'

[15] Stewart Patrick, 'World order: what exactly are the rules?', *Washington Quarterly* 39: 1, 2016, p. 8; Beate Jahn, 'Liberal internationalism: historical trajectory and current prospects', *International Affairs* 94: 1, Jan. 2018, pp. 43–62; Inderjeet Parmar, 'The US-led international order: imperialism by another name', *International Affairs* 94: 1, Jan. 2018, pp. 151–72.

[16] Mary Kaldor, *New and old wars: organized violence in a global era*, 2nd edn (Cambridge: Polity, 2006).

[17] Hanns Maull, ed., *The rise and decline of the post-Cold War international order* (Oxford: Oxford University Press, 2018); Amitav Acharya, 'After liberal hegemony: the advent of a multiplex world order', *Ethics and International Affairs* 31: 3, 2017, pp. 271–85; Graham Allison, 'The myth of the liberal order. from historical accident to conventional wisdom', *Foreign Affairs* 97: 4, July–Aug. 2018, pp. 124–33.

[18] Constance Duncombe and Tim Dunne, 'After liberal world order', *International Affairs* 94: 1, Jan. 2018, p. 25.

[19] Olivier Stuenkel, *Post-western world* (Cambridge: Polity, 2016).

[20] Fareed Zakaria, *The post-American world* (London and New York: Norton, 2008).

in the US leadership.[21] The **{2}** 'post-' prefix in all these expressions highlights the transitory dimension of the current era, and the uncertainty surrounding its direction. Other debates focus more on the challenges to the multilateral system, with deadlock hampering some existing institutions (UN, WTO) and new ones coming into existence, for example the Shanghai Cooperation Organization (SCO), Asian Infrastructure Investment Bank (AIIB).[22] In yet other discussions, the focus is on the loss of traction of liberal norms and values, and the rise of certain forms of 'illiberalism'.[23]

Although it is debatable whether the world can already be called 'multipolar' (or whether we can justifiably speak of the decline of the West),[24] it is becoming increasingly clear that the US unipolar moment is over. China has become a competing Great Power, or at the very least an unavoidable stakeholder or, as the Germans say, a shaping power (*Gestaltungsmacht*), that is, a state that has power to influence global issues and debates. Other countries lack the same level of power, but are able to make use of their resources (including in the cyber realm) to gain a certain form of negative power, or power of denial.[25] The exact polar configuration of this potentially new world order is still unclear, but the current configuration certainly involves a variable geometry, with states wielding **{3}** different degrees of power and influence across different issues or regions.

Looking only at the global chessboard of power politics may be misleading, however. Power is not an absolute quantity that is merely transferred from one country to another, or from the

[21] Duncombe and Dunne, 'After liberal world order', p. 27.

[22] Shahar Hameiri and Lee Jones, 'China challenges global governance? Chinese international development finance and the AIIB', *International Affairs* 94: 3, May 2018, pp. 573–94; Martin Hearson and Wilson Prichard, 'China's challenge to international tax rules and the implications for global economic governance', *International Affairs* 94: 6, Nov. 2018, pp. 1287–1308.

[23] For an early discussion of the topic, see Fareed Zakaria, 'The rise of illiberal democracy', *Foreign Affairs* 76: 6, Nov.–Dec. 1997, pp. 22–43.

[24] Michael Cox, 'Power shifts, economic change and the decline of the West?', *International Relations* 26: 4, 2012, pp. 369–88.

[25] Mark Galeotti, *Heavy metal diplomacy: Russia's political use of its military in Europe since 2014*, policy brief (London: European Council on Foreign Relations, Dec. 2016), https://www.ecfr.eu/publications/summary/heavy_metal_diplomacy_russias_political_use_of_its_military_in_europe_since.

West to the East (or 'the rest').[26] Several countries are rising together without necessarily triggering the decline of the United States or Europe. The shift of power that characterizes the post-liberal order is complex and often unpredictable. Power is shifting not only horizontally, but also vertically. We are dealing with a broader and arguably more structural phenomenon of power moving away from states and concentrating in other actors that have a real capacity to influence and change social reality. For Anne-Marie Slaughter, this trend can be encapsulated in the distinction between the world as a chessboard, in which foreign policy experts analyse 'the decisions of great powers and anticipat[e] rival states' reactions in a continual game of strategic advantage', and the world as a web, composed not merely of states, but also of networks of multiple actors, from NGOs to multinational corporations.[27] In this environment, states need to adjust their role: they must be 'waves and particles at the same time',[28] that is, they remain the main actors in issues of international security, but they are also the hubs for multiple transnational activities—legal and illegal alike—'that reverberate in global affairs just as much as state actions do'.[29] This view is shared by other authors. For instance, Richard Haass claims we are now living a 'world order 2.0', built on increasing transnational dynamics,[30] in which 'the inadequacies of the traditional approach to order, based on sovereignty alone, will only become more obvious over time.'**{5}**[31] Joseph Nye Jr concurs, arguing that 'governments will continue to possess power and resources, but the stage on which they play will become ever more crowded, and they will have less ability to direct the action'.[32] The second key dimension of the post-liberal order is the growing contestation and retreat of the so-called liberal values. Democracy (and all the values that underpin it, such as human rights and freedom of expression or press), which is arguably the core value of the liberal order,

[26] Yuen Foong Khong, 'Power as prestige in world politics', *International Affairs* 95: 1, Jan. 2019, pp. 119–42.

[27] Anne-Marie Slaughter, 'How to succeed in the networked world: a grand strategy for the digital age', *Foreign Affairs* 95: 6, 2016, p. 76.

[28] Slaughter, 'How to succeed in the networked world', p. 87.

[29] Slaughter, 'How to succeed in the networked world', p. 87.

[30] Richard Haass, 'World order 2.0: the case for sovereign obligation', *Foreign Affairs* 96: 1, Jan.–Feb 2017, pp. 2–9.

[31] Haass, 'World order 2.0', p. 9.

[32] Joseph Nye Jr , 'Will the liberal order survive? The history of an idea', *Foreign Affairs* 96: 1, Dec. 2016, p. 14.

is under pressure. The wave of democratization that took place in the late twentieth century has clearly stopped.[33] China and Russia are, in Michael Mazarr's words, the 'two most important dissenters' of our current order:

> Both countries feel disenfranchised by a US-dominated system that imposes strict conditions on their participation and, they believe, menaces their regimes by promoting democracy. And both countries have called for fundamental reforms to make the order less imperial and more pluralistic.[34]

Their calls for multipolarity and pluralism are also pleas for a recognition of the relativity of norms and values, and the abandoning of so-called 'universal principles'.[35]

Liberal values are under challenge not merely from so-called 'illiberal powers', but also internally. As John Ikenberry points out, 'for the first time since the 1930s, the United States has elected a president [Donald Trump] who is actively hostile to liberal internationalism'.[36] Similar cases are noticeable in Europe—in Hungary or Poland, for instance. In contrast, 'illiberal' China sought to present itself as the beacon of globalization at the 2017 World Economic Forum, and has arguably been keen to avoid escalating a trade war with the United States which could potentially lead to the demise of the WTO system. Overall, this twisting of liberal rules and values—from the inside and the outside—is progressively affecting, if not eroding, the meaning of the liberal order.

The third and last dimension through which the liberal order is being challenged relates to the rules-based multilateral system. The UN, the Bretton Woods institutions and the WTO are traditionally associated, if not simply equated, with the liberal order, as they aim for global

[33] Michael J. Abramowitz, *Freedom in the world 2018: democracy in crisis* (Washington and New York: Freedom House, 2018), https://freedomhouse.org/report/freedom-world/freedom-world-2018.

[34] Michael J. Mazarr, 'The once and future order', *Foreign Affairs* 96: 1, Jan.–Feb 2017, p. 27.

[35] See Amitav Acharya, 'After liberal hegemony: the advent of a multiplex world order', *Ethics and International Affairs* 31: 3, Fall 2017, pp. 271–85; also Charles Kupchan, *No one's world* (Oxford: Oxford University Press, 2012).

[36] Ikenberry, 'The end of liberal international order?'. Trump even objected to the expression 'the rules-based order' in the 2018 G7 summit statement: see Peter Baker, 'Escalating clash with Canada, Trump is isolated before North Korea meeting', *New York Times*, 10 June 2018, https://www.nytimes.com/2018/06/10/us/politics/trump-trudeau-summit-g7-north-korea.html.

membership and promote norms and values that are deemed ‘liberal’ and ‘universal’: as Kahler has pointed out, they are ‘globalizers’.[37] The contestation of these institutions is not new. The so-called ‘Washington consensus’ promoted by the Bretton Woods institutions was heavily criticized in the 1980s and 1990s. In the UN context, many countries have long been dissatisfied with the non-democratic composition of the Security Council, with its five permanent members. Over the past decade, emerging powers—most of which are not properly represented in the western-dominated multilateral system—have increased their pressure to reform the multilateral system with a view to adjusting it to reflect their new status.[38] In 2010 they negotiated a reform of voting shares in the IMF and World Bank, and they have also become much more active and influential in the multilateral system (for example, in the UN General Assembly, in UN climate talks and in WTO talks).[39] It is important to note that, in promoting the reform of the multilateral institutions, they also evince their support of these institutions. Reform is certainly different from overthrowing, and so far, neither China nor Russia seems to have either the urge or the capacity to promote the latter, or to offer a grand ideological alternative to the current institutional set-up.[40]

Cyberspace is not immune to these dynamics; indeed, they are particularly salient within this realm. In the next two sections we analyse how these scenarios pan out in cyberspace by looking at power, values and institutional dynamics within it.

The post-liberal cyberspace

Given its growing use for political purposes, cyberspace is inevitably affected by post-liberal trends. Beginning with the first of the three main dimensions mentioned above – power –, we understand cyber power as ‘the ability to use cyberspace to create advantages and influence

[37] Miles Kahler, ‘The global economic multilaterals: will eighty years be enough?’, *Global Governance*, 22: 1, 2016, pp. 1–9.

[38] Nele Noesselt, ‘Contested global order(s): rising powers and the re-legitimation of global constitutionalization’, *International Journal of Constitutional Law* 14: 3, July 2016, pp. 639–56.

[39] See Kathryn Hochstetler and Manjana Milkoreit, ‘Responsibilities in transition: emerging powers in the climate change negotiations’, *Global Governance* 21: 2, Aug. 2015, pp. 205–26; Kristen Hopewell, ‘The BRICS—merely a fable? Emerging power alliances in global trade governance’, *International Affairs* 93: 6, Nov. 2017, pp. 1377–96.

[40] Ikenberry, ‘The end of liberal international order?’, p. 23.

events in other operational environments and across the instruments of power'.[41] That can be accomplished either within cyberspace or through the use of cyber instruments to achieve results in the kinetic realm.[42] Such definition includes a state's capacity to conduct aggressive cyber operations (or to deter or withstand such operations), its ability to influence the international cyber agenda, and its ability to use cyber (including information) tools to promote a broader agenda and wider interests. According to Adam Segal, great cyber powers combine four components: 'large or technologically advanced economies; public institutions that channel the energy and innovation of the private sector; adventurous and somewhat rapacious military and intelligence agencies; and an attractive story to tell about cyberspace'. Only a few countries would indeed qualify as great cyber powers. The United States remains the equivalent of the lonely cyber superpower, although China and Russia are progressively catching up and are relatively more powerful than in any other domain.[43]

Beyond the balance of power, cyberspace is becoming a major factor in the shifting global pecking order for two other reasons. First, the 'cyber' dimension of power is increasingly central to the very definition of power, whether in economic or security terms, with the growing share of the digital economy in global trade and innovation, and the digitalization of security. Second, cyber capabilities are increasingly becoming a means by which countries can compensate for their lesser power in other domains. This allows small nations (such as Estonia and Singapore) to punch above their weight, and enables mid-level powers (such as Israel, Iran and North Korea) to catch up more rapidly with established powers through the integration of cyber tools in military hybrid doctrines, as well as, in some cases, through the use of cyber tools to steal technological secrets. As a result, it is not surprising that states across the world are increasingly interested in developing their cyber capacities across the whole power spectrum.[44]

[41] Daniel T. Kuehl, 'From cyberspace to cyberpower: defining the problem', in Franklin D. Kramer, Stuart Starr and Larry K. Wenz, eds), *Cyberpower and national security* (Washington: National Defense University Press, 2009), p. 38.

[42] Joseph Nye Jr, *Cyber power* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010), p. 4.

[43] Segal, *The hacked world order,* p. 34.

[44] Segal, *The hacked world order*; Alexander Klimburg, *The darkening Web: the war for cyberspace* (London and New York: Penguin, 2017).

Cyberspace itself is evolving to become less western-centric, and more 'post-liberal'. Non-western countries are emerging as cyber powers, and some of today's largest tech companies are in Asia.[45] Furthermore, the internet infrastructure and users are increasingly located outside the West. The most connected country in the world is now South Korea, while the share of individuals connected to the internet in Asia grew from 34 per cent of the global share in 2005 to just above 50 per cent in 2016**{6}**.[46] In terms of absolute numbers**{7}**, there are more internet users in Asia than in the rest of the world, and technological developments seem to be gaining pace in the region. 5G and artificial intelligence (AI) are two areas in which China, in particular, seems to be taking the lead, potentially making cyberspace ever less western.[47]

As noted above, a key aspect of the post-liberal order is the articulation between the world as a chessboard and the world as a web.[48] Non-state actors are central to the latter, particularly in cyberspace, where they have been dominant players. Increasingly, major internet companies are also inevitable interlocutors in national or international legislative work over cyberspace. This was visible in their lobbying efforts in Brussels over data protection.[49] The same applies to the fight against online terrorism and extremism, where some technology and social media companies have become major stakeholders and also powerful policy-shapers through dedicated platforms, such as the Global Internet Forum to Counter Terrorism (GIFCT) or the EU Internet Forum. Beyond the IT world, insurance companies are also starting to play an important role as promoters of a stable cyberspace. There is the expectation that they will be

[45] According to Forbes' list of largest tech companies 2018, Asia had three companies (Samsung, Tencent and Hon Hai Precision Industry) in the global top ten. For more information, see: https://www.forbes.com/sites/kristinstoller/2018/06/06/worlds-largest-tech-companies-2018-global-2000/#6dae455d4de6.

[46] Information available at https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[47] Michael Woolridge, 'China challenges the US for artificial intelligence dominance', *Financial Times*, 15 March 2018, https://www.ft.com/content/b799cb04-2787-11e8-9274-2b13fccdc744; Andrew B. Kennedy and Darren J. Lim, 'The innovation imperative: technology and US–China rivalry in the twenty-first century', *International Affairs* 94: 3, May 2018, pp. 553–72.

[48] Slaughter, 'How to succeed in the networked world'.

[49] Monica Holten, *The closing of the internet* (Cambridge: Polity, 2016).

on the front line in the promotion of common norms and standards in cyberspace.[50] Related to this is the phenomenon we have been witnessing in the past few years whereby some of these actors have been attempting to play an active role on the diplomatic chessboard as norm entrepreneurs.[51] For instance, Microsoft proposed a 'Digital Geneva Convention' at the RSA conference in San Francisco in February 2017;[52] more recently, it sponsored the creation of the CyberPeace Institute,[53] and signed the 'Cybersecurity Tech Accord' with 33 other companies––in which they set out four key principles,[54] with the ultimate aim of protecting technology users across the globe. Microsoft sees itself as having 'an obligation to protect civilians' in cyberspace[55]—an idea with which some states are not entirely comfortable, seeing it as impinging on their sovereign and international rights and responsibilities.

With regard to values in the post-liberal order, cyberspace is at the centre of two major and complex debates. One concerns the relation of the concept of cybersecurity to that of information security. The other concerns the libertarian ideal of a free and open internet and is articulated around the possibility of its fragmentation.

While most western governments talk about 'cyber security', a number of nations prefer the term 'information security'.[56] Behind a seemingly benign semantic distinction lies a significant

[50] Joseph S. Nye, *Normative restraints on cyber conflict* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2018), p. 22.

[51] Louise Mariel Hurel and Luisa Cruz Lobato, 'Unpacking cyber norms: private companies as norm entrepreneurs', *Journal of Cyber Policy* 3: 1, **2018,** pp. 61–76.

[52] Brad Smith, *The need for a digital Geneva Convention: Microsoft on the issues*, 14 Feb. 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[53] For more information see: https://cyberpeaceinstitute.org/.

[54] The key principles are: (1) to protect all users and customers everywhere; (2) to oppose cyber attacks on innocent citizens and enterprises from anywhere; (3) to empower users, customers and developers to strengthen cyber-security protection; and (4) to partner with each other and with like-minded groups to enhance cyber security. For more information, see https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/.

[55] Author's interview with Microsoft representative, Brussels, May 2018.

[56] Russia's 2016 Doctrine of Information Security defines the information sphere as the 'combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet . . ., communication

clash of views on the future of cyberspace. Russia and China have actively promoted information security in international talks, using a term that is widely employed by the technical community but changing its traditional meaning to reflect Moscow's and Beijing's attempts to legitimize a greater control over all aspects of information flows.[57] A considerable part of rising powers' unease about cyberspace has to do with the danger they perceive from the free flow of information.[58] The semantic distinction is not restricted to that between cyber security and information security. Concepts such as 'multistakeholder', 'democracy' and 'multilateralism' are all employed differently by different actors. According to Joseph Nye, the Chinese delegation at the Fourth World Internet Conference, which took place in 2017 at Wuzhen in China, defended 'an open Internet subject to sovereignty'; but their understanding of an 'open internet' was very different from that proposed by the Freedom Online Coalition.[59]

The second debate has to do with internet freedom. According to the 2018 Freedom on the Net report by Freedom House, global internet freedom has declined for the eighth consecutive year as the result of an increase in practices of disinformation and propaganda, infringements of privacy and the overall rise of 'digital authoritarianism'.[60] Internet content control is commonly understood to be an issue of global relevance, notably in the context of countering extremist

networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere': Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation* (Moscow, 5 Dec. 2016), Available at: http://www.scrf.gov.ru/security/information/DIB_engl/ **{?}**.

[57] Klimburg, *The darkening Web*, p. 118. See also Adam Segal, *Chinese cyber diplomacy in a new era of uncertainty*, Aegis Paper no. 1703 (Stanford, CA: Hoover Institution, June 2017); Hannes Ebert and Tim Maurer, 'Contested cyberspace and rising powers', *Third World Quarterly* 34: 6, July 2013, pp. 1054–74; Yevgeniy Golovchenko, Mareike Hartmann and Rebecca Adler-Nissen, 'State, media and civil society in the information warfare over Ukraine', *International Affairs* 94: 5, Sept. 2018, pp. 975–994.

[58] Ebert and Maurer, 'Contested cyberspace and rising powers'.

[59] Joseph Nye, *Normative restraints on cyber conflict*, p. 12.

[60] Adrian Shabaz, *The rise of digital authoritarianism* (Washington and New York: Freedom House, Oct. 2018), https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

propaganda and other problematic material. In this respect, the slope towards 'information security' is quite slippery and the line between freedom and censorship quite fine: while everyone agrees that paedophile pornography should be banned, the banning of extremist content comes up against several hurdles (What is 'extremist content'? What is an 'extremist group'?), while the fight against disinformation and 'fake news' opens many Pandora's boxes.[61]

There is a broad division between those countries that emphasize the importance of an 'open and free internet', and those that defend the principle of 'cyber sovereignty' and the need to maintain public order in cyberspace.[62] Authoritarian states have always been wary of data and information flows in their concern to protect incumbent regimes and domestic stability. They were, therefore, active in developing national regulations (such as China's famous Great Firewall or Iran's Halal Net) or to promote global ones in line with their own concerns. In contrast, western states have always vocally promoted a 'free and open internet'. However, beyond the clash of principles between these two visions, the reality has historically been more nuanced: within the West, the origins of internet governance were ridden with divisions between Americans and Europeans, but also between the White House and those at the forefront of the creation of the internet.[63] As Milton Mueller argues, the focus should not be on 'fragmentation', but rather on the alignment of internet services along national borders. Already, indeed, not all content can be accessed from all locations.[64] As Mueller points out,

[61] Ian Klinke, 'Geopolitics and the political right: lessons from Germany', *International Affairs* 94: 3, May 2018, pp. 495–514.

[62] Cyber sovereignty was defined by Xi Jinping as 'the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing'. Quoted in Adam Segal, 'When China rules the Web', *Foreign Affairs* 97: 5, Sept.–Oct. 2018, pp. 10–18.

[63] This was particularly the case with the creation of the Internet Corporation for Assigned Names and Numbers (ICANN). For more, see Milton Mueller, 'ICANN and internet governance: sorting through the debris of "self-regulation"', *Information and Media* 1: 6, 1999, pp. 497–520.

[64] Martina F. Ferracane, *Restrictions on cross-border data flows: a taxonomy*, ECIPE working paper no. 1 (Brussels: European Centre for International Political Economy, 2017);

what we have is 'a power struggle over the future of national sovereignty in the digital world. It's not just about the Internet. It's about geopolitics, national power, and the future of global governance.'[65] Here power, values and institutions converge.

Finally, with regard to institutional change, a number of nations are challenging existing cyber regimes, including in the field of internet governance. Rising powers have contested decentralized governance models on the grounds that they give too much power to private actors and not enough to governments. Instead of the multistakeholder model,[66] they prefer an intergovernmental model, which they claim is more 'democratic and pluralistic'. They also advocate a much more significant role for the International Telecommunication Union (ITU), a UN agency, in regulating the internet.[67]

In the post-liberal era, rising powers are asking for more representation and power in internet governance; but in the West as well, the trend towards more state control over the internet is challenging the status quo of the multistakeholder model. Over the past decade, a number of international forums have emerged (such as the ITU's World Summit on the Information Society, or China's sponsored World Internet Conference) which share the aim of giving more power over cyberspace, and in particular over the internet, to governments.[68] As Mueller argues, 'a state-centric approach to global governance cannot easily co-exist with a multistakeholder regime. Fundamentally, they are in competition; one or the other must prevail in the domain of Internet governance.'[69]

Council on Foreign Relations, *The rise of digital protectionism*, insights from a CFR workshop (New York, 18 Oct. 2017).

[65] Milton Mueller, *Will the internet fragment? Sovereignty, globalization and cyberspace* (Cambridge and Malden, MA: Polity, 2017), p. 3.

[66] Embodied in ICANN, a non-profit organization with administrative responsibilities regarding the internet's global domain name system, which is composed of a multiplicity of stakeholders, from IT experts to government representatives (in an advisory role).

[67] Robert Mogus, Jocelyn Woolbright and Justin Sherman, *The digital deciders*, New America Cybersecurity Initiative (Washington DC: New America, Oct. 2018), p. 14, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

[68] Although there is a degree of overlap between the internet and cyberspace, the latter goes beyond the former, including information networks that may not be directly linked the network of networks.

[69] Mueller, *Will the internet fragment?*, p. 117.

‘Illiberal’ states such as Russia and China have strategically sought to move internet governance debates under the aegis of the UN, in order to ‘prioritize the interests of governments over those of technology companies and civil society groups’, and this approach does have**{9}** the support of developing countries.[70] Putin has made clear that he and his allies seek to establish through the ITU ‘international control over the internet’.[71]

Differences also abound when it comes to security in cyberspace. Even on cybercrime, an area that is slightly less divisive, consensus is elusive. The Budapest Convention, to date the closest there is to an international legally binding cyber-security treaty, has not been signed by all the Council of Europe members, most importantly by Russia.

Overall, cyberspace is increasingly competitive, fragmented and disordered. Order in cyberspace, as in the physical world, does not come about by itself. Most discussions on global order often overlook the amount of effort needed to transform a ‘balance of power’ into a functioning and institutionalized order—even if that order has only minimal rules (such as the Cold War order). In these efforts, diplomacy plays a crucial role as a ‘primary institution’ of international society.[72] As we shall see in the next section, if one assumes—as we do—that diplomacy is a fundamental institution in the creation and maintenance of any given international order,[73] then cyber diplomacy must be expected to be prominent in the post-liberal transition of order in cyberspace. The question is how and to what extent.

Cyber diplomacy as a post-liberal practice

As recent academic works have emphasized, the growing politicization of cyberspace has generated a significant diplomatic interest and a proliferation of initiatives in this realm.[74]

[70] Adam Segal, ‘When China rules the Web’.

[71] Robert M. McDowell, cited in Mirko Hohmann and Thorsten Benner, *Getting ‘free and open’ right: how European internet foreign policy can compete in a fragmented world*, policy paper (Berlin: Global Public Policy Institute, June 2018), p. 15.

[72] Duncombe and Dunne, ‘After liberal world order’; Inis Claude, *Power and international relations* (New York: Random House, 1962).

[73] Hedley Bull, *The anarchical society: a study of order in world politics,* 3rd edn (Basingstoke: Palgrave Macmillan, 2002).

[74] Barrinha and Renard, ‘Cyber-diplomacy’; Thomas Renard, ‘EfU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain’, *European Politics and Society* 19: 3, 2018, pp. 321–37; Shaun Riordan, *Cyberdiplomacy: managing security and governance online* (Cambridge: Polity, 2019).

Starting essentially in the early 2010s, a growing number of countries have published foreign policy strategies for cyberspace, appointed 'cyber diplomats' and become more active on cyber issues in international forums—which have themselves multiplied (including the World Summit on the Information Society, the World Internet Conference**{10}**, and the London process). In this section, we look at the role of cyber diplomacy in either strengthening or resisting post-liberal trends, and contributing to order through various functions of diplomacy, which together range over the three dimensions reviewed above (power, values and institutions).

First, at the most basic level, cyber diplomacy is essential to keep channels of communication open between states, and also between states and international organizations, civil society and non-state actors**{11}**. As noted above, non-state actors have historically played a primary role in the shaping of the internet and its governance. This was not particularly remarkable at a time when cyberspace was for the most part apolitical. However, the growing politicization of cyberspace has engulfed non-state actors in the international politics of cyberspace. As Shaun Riordan argues, if one accepts diplomacy as a 'way of being in the world' defined by 'common attitudes and ways of seeing and interacting with international issues', then non-state actors could be seen as diplomatic actors as long as they 'shared in these common ways of acting with or thinking about the world'.[75]

Furthermore, a growing number of states are increasing their interest in cyberspace, developing policies and strategies that denote specific understandings of how cyberspace should be governed, nationally and internationally. In an increasingly crowded field, with diverse and often divergent views encompassing states and non-state actors, cyber diplomacy has become essential to keep track of all these developments. While the nomination by Denmark of the world's first 'Tech Ambassador' in 2017, with an office in Silicon Valley, is certainly an illustration of this, the recent tensions between the United States, Europe and China over the transition to 5G network technology, and the role of the Chinese company Huawei therein, is perhaps even more telling: what was first a technical dossier became highly politicized and eventually securitized, requiring intense diplomatic discussions.

Second, cyber diplomacy seeks to prevent or mitigate the potentially negative consequences of offensive actions in cyberspace. Over 30 countries are openly pursuing defensive and offensive cyber capabilities (these include**{12}** China, India, Russia, South Africa, South Korea, Iran and

[75] Riordan, *Cyberdiplomacy,* p. 23.

North Korea), and a dozen more are likely to be heading in that direction.[76] Malicious activities can also include a form of 'information warfare': the ability of countries such as China and Russia to use digital tools to influence their image and global opinions is well documented. As Ashley Coward and Corneliu Bjola have noted, state responses to growing cyber competition and insecurity have for the most part focused on developing more capabilities, notably offensive ones, hence reinforcing global insecurity, instead of pursuing 'more open and cooperative responses'.[77] Cyber diplomacy is necessary to guarantee that offensive cyber activities are limited in scope and nature, and that they do not lead to unnecessary escalation or mis-attribution. In 2015, China and the United States signed an agreement in which both made a commitment not to use cyberspace for economic espionage purposes, and in subsequent months there was a significant (albeit temporary) reduction in terms of Chinese cyber activity against US companies in subsequent months, suggesting that such agreements can work.[78]

Third, more constructively, cyber diplomacy is fundamental for the development of global norms and standards at the regional and international levels. This touches on the issue of the applicability of international law to cyberspace. Since 2004, a UN Group of Government Experts (GGE) on Developments in the Field of Information and Communications Technologies in the Context of International Security has met to discuss and reach decisions on issues pertaining to the norms regulating cybersecurity. The process followed from a Russian proposal in 1998 for a UN treaty to ban electronic and information weapons. The long title of the group was formulated to incorporate both Russia's interest in 'information security' and that of the United States in 'cyber operations'.[79] It was the efforts of the previous UN GGE **{13}** that led to a recognition that existing international law applies to cyberspace, and that there is therefore no need for an entirely new form of law. However, the extent to which, and the manner in which, existing laws apply in cyberspace is still open to debate, and is a topic in

[76] Klimburg, *The darkening of the Web*, p. 301.

[77] Ashley Coward and Corneliu Bjola, 'Cyber-intelligence and diplomacy: the secret link', in Corneliu Bjola and Stuart Murray, eds, *Secret diplomacy: concepts, contexts and cases* (London: Routledge, 2016), pp. 201–28.

[78] Alex Grigsby, *The United Nations doubles its workload on cyber norms, and not everyone is pleased* (New York: Council on Foreign Relations, Nov. 2018), p. 25, https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

[79] Joseph S. Nye, *Normative restraints on cyber conflict*, p. 9.

continuing discussions. While there is a degree of consensus among certain actors, notably in the West as illustrated by the two Tallinn manuals,[80] its reach is far from global. Indeed, there have been five UN GGEs on this topic since 2004, three of which have reached consensus reports (in 2010, 2013 and 2015). No consensus could be found in 2017, owing to divergences on 'the future of the global information space and the principles by which it will be regulated', according to Andrey Krutskikh, Russia's Special Representative for International Cooperation on Information Security.[81] In his official statement, Krutskikh contrasted Russia's 'peace-oriented concept' with 'the position of certain countries that seek to impose on the whole world their own game rules in the information space'.[82] By contrast the US representative, Michelle Markoff, attributed the failure to reach a consensus to 'the reluctance of a few participants to seriously engage on the mandate on international legal issues'.[83]

Discussions within the First Committee of the UN General Assembly gained momentum in September and October 2018, leading to the proposal of new initiatives at the UN level. However, rather than leading to a consensual new approach, the outcome revealed a clear

[80] Michael N. Schmitt, ed., *Tallinn manual on the international law applicable to cyber warfare* (Cambridge: Cambridge University Press, 2013); Michael N. Schmitt, ed., *Tallinn manual 2.0 on the international law applicable to cyber operations* (Cambridge: Cambridge University Press, 2017).

[81] Ministry of Foreign Affairs of the Russian Federation, 'Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' question concerning the state of international dialogue in this sphere', 29 June 2017, http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288.

[82] The Ministry of Foreign Affairs of the Russian Federation, 'Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere' (Moscow, 29 June 2017), http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288.

[83] Elaine Korzak, 'UN GGE on cybersecurity: the end of an era?', *The Diplomat,* 31 July 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

international division on how to proceed in terms of the international regulation of cyberspace. Although Russia initially tabled a motion proposing a new GGE, it eventually replaced it with the more expansive format of an Open-Ended Working Group (OEWG)**{14}**. This allowed Russia to place itself 'as an advocate of democratic participation and inclusivity'.[84] Two different draft resolutions were then put on the table: A/C.1/73/L.37, proposed by 36 states (including the United States and the EU member states); and A/C.1/73/L.27 proposed by 27 states (including Russia and China). This means that there are now two parallel groups, with partially overlapping membership, discussing very similar issues during the same period. The GGE includes 25 selected members, whereas the OEWG is open to all interested countries and includes consultations with non-state actors.[85]

The setting up of two parallel forums within the UN General Assembly can be seen as a failure for cyber diplomacy. However, the decision to go with two different proposals was made only after attempted negotiations between Russia and western countries. **{15}** Furthermore, even if the twin-track process that led to the current situation in the General Assembly could be seen as a crystallization of existing international divisions, when it comes to cyberspace both China and Russia participate as permanent members of the Security Council and in the GGE meetings, and all**{16}** the GGE members are allowed to contribute to the OEWG. In short, at the multilateral level, there are multiple layers of discussions with partial overlap, rather than a clear-cut fracture between opposing sides. These parallel tracks, along with the multiplication of multilateral and transnational forums, highlight the need for more diplomacy. This need is felt both in practical terms—the need for people to participate in all these meetings—but also in strategic terms, so that the major stakeholders are able to offer clear and consistent positions, using these events to generate a continuous dialogue with concrete aims.

Finally, cyber diplomacy is, for states, about promoting their respective interests and visions for global order, and gathering the widest support possible for those positions. We have already mentioned the deep divisions among nation-states over core issues of internet policies. This

[84] Grigsby, *The United Nations doubles its workload*.

[85] As Alex Grigsby explains: 'Procedurally, GGEs have a smaller membership—previous cyber GGEs had anywhere between fifteen and twenty-five participants—and have time-bound mandates, which theoretically curb diplomats' urge to kick the can down the road. By contrast, OEWGs have much bigger memberships—any of the 193 UN member states can participate in its deliberations, and their open-ended nature means that they can go on forever or until member states agree to dissolve it' (*The United Nations doubles its workload*).

was already visible in 2012, during a vote at the World Summit on the Information Society, which largely split countries into two distinct camps.[86] As a result of this experience, some countries have been identified as potential ‘swing states’,[87] which could be persuaded to switch sides or form a bridge between extreme views.[88] In such endeavours, narratives matter tremendously. The Chinese and Russian narrative on ‘cyber-sovereignty’ has become increasingly compelling for a number of non-western states (and also for some western ones) in the post-liberal era. In contrast, the western narrative of a ‘free and open internet’, in times of internet content regulation and digital protectionism, sound increasingly hollow, if not hypocritical.[89] In spite of these distinctly different visions, the more nuanced reality of a de facto fragmented internet opens up space for a *rapprochement* between the different stakeholders.

In this respect, cyber diplomacy appears crucial for the stabilization of the vocabulary in international cyberspace policy, in which the same specific terms can refer to sharply different visions for cyberspace. As in other spheres of international life, it is unlikely that a shared language will necessarily reduce the cultural differences between the main stakeholders, but it is an essential preliminary step towards building mutual comprehension and a shared vision for cyberspace. One of cyber diplomacy’s roles is to be capable of providing the necessary translation of those concepts across states and cultures.[90]

As mentioned earlier, diverging preferences and visions have also led to a proliferation of competing institutional forums to discuss cyber issues. Some of these institutions are state-led, such as ITU; others are led by civil society, such as the Global Commission on the Stability of

[86] Madeline Carr, ‘Power plays in global internet governance’, Millennium: Journal of International Studies, 43:2, 2015, pp. 648–50.**{?}**

[87] A ‘swing state’ is a state ‘whose mixed political orientation gives it a greater impact than its population or economic output might warrant and that has the resources that enable it to decisively influence the trajectory of an international process’: Tim Maurer and Robert Morgus, *Tipping the scale: an analysis of global swing states in the internet governance debate*’ (London: Centre for International Governance Innovation and Chatham House, May 2014), p. 4.

[88] Maurer and Morgus, *Tipping the scale*.

[89] Hohmann and Benner, *Getting ‘free and open’ right,* p. 8.

[90] Author’s interviews with European External Action Service official, **Brussels,** May 2018, and with UK Foreign and Commonwealth Office official, London, June 2018.

Cyberspace; most follow some kind of multistakeholder model.[91] Some countries, notably China, have also launched new multilateral initiatives, such as the World Internet Conference beginning in 2014, which not only add to the many existing ones but, to some extent, also compete with them, through the offer of a China-centric model. This has two consequences. First, it makes it difficult to concentrate efforts and resources; from a cyber diplomat's perspective, there is a lot of redundancy and loss of focus in this multiplicity of encounters. Second, it both helps and hinders norm-building exercises. In interviews with officials from both the EU and European states, it was mentioned that the diversity of actors involved allows for a richer dialogue about these issues. Interviewees were, however, well aware of the difficulty in translating that dialogue into concrete outcomes. In the current context, keeping the conversation going seems to be the best that can be achieved.[92]

Cyber diplomacy: building order or bridges?

The American-led liberal order created the necessary conditions for inventors, ideas and institutions to develop information networks connected at a global scale. It also set the technical standards and provided the necessary impetus for the creation of decentralized multistakeholder-based governance institutions. As this article has argued, if the development of cyberspace was enabled by the liberal order, cyber diplomacy's *raison d'être* is firmly situated in the current post-liberal transition. Cyber diplomacy has developed organically, accompanying the increasing salience of cyberspace across the world and its increasing strategic importance.

Cyber diplomacy is both a response to and a factor in the continuing battle for influence in and over cyberspace. The dynamics at work here are very much along the lines of those we observe in the kinetic dimension of the post-liberal order, with values and institutions at the centre of a power struggle between multiple states and non-state actors. However, unlike diplomacy in the kinetic world, the international practice of cyber diplomacy is a fairly recent one. As Deborah Housen-Couriel calculated in her study of diplomatic initiatives in cyberspace, out of the 84 initiatives identified, 83 per cent have been developed since 2012, and more than half (63 per

[91] Laura DeNardis and Mark Raymond, 'Thinking clearly about multistakeholder internet governance', paper presented at the Eighth Annual GigaNet Symposium, Bali, Indonesia, 21 Oct. 2013.

[92] Mueller, *Will the internet fragment?,* p. 111.

cent) in 2015 or later.[93] Given the speed at which developments in the field are taking place, and with the increasing attention paid by states and private actors to what is happening in cyberspace, cyber diplomacy as a field of research is in need of far greater academic attention. Although the international relations of cyberspace do not take place in a vacuum, isolated from what goes on in other spheres of international politics, the novelty of the field opens up the possibility for the establishment of new international and transnational dynamics and relationships. States that pull above their weight in cyberspace will be able to see their views taken into consideration by the main powers of the international system. Digital companies will be able to establish alliances and partnerships with companies and states with which they share common interests. This will all happen in a context marked by the increasing complexity of the field, with the internet of things dramatically increasing the vulnerability of states and companies, and AI changing the defensive and offensive landscape in cyberspace, through automated and self-developed responses to network threats. As Shaun Riordan argues, the rise of AI will also have implications for diplomacy itself, both in terms of using algorithms for conflict resolution and more mundanely, automating many of the bureaucratic responsibilities associated with the job.[94] Technology will certainly make the context in which cyber diplomacy operates more complex, which in turn makes it even more important to follow developments in this domain closely.

As this article has shown, power, values and institutions are in flux, both in the kinetic world and in cyberspace. From the literature on the (post-)liberal order, we have established that there is a tension resulting from the fact that the liberal order no longer reflects the balance of power, values and institutional preferences of emerging powers and powerful non-state actors, leading to a contestation of this order. As Noesselt puts it, there is a tension between the *pouvoir constitué* and the *pouvoir constituant.*[95]

Following Miles Kahler, one could argue that there are three main possible scenarios to deal with this contestation in the kinetic world:[96] reform, disengagement or fragmentation. *Reform* means that a compromise is found between the main powers of the international system,

[93] Deborah Housen-Couriel, ‘An analytical review and comparison of operative measures included in cyber diplomatic initiatives’, briefing from the Research Advisory Group, Global Commission on the Stability of Cyberspace, New Delhi, Sept. 2017, p. 61.

[94] Riordan, *Cyberdiplomacy,* p. 109.

[95] Noesselt, ‘Contested global order(s)’, p. 640.

[96] Kahler, ‘The global economic multilaterals’.

essentially preserving the existing institutions but providing more space for rising powers. *Disengagement* means that rules-based multilateralism loses traction and the international system becomes a zero-sum game. In other words, it is not only the multilateral institutions that are being challenged, but multilateralism as such. This is a world of intense competition and bargaining, with limited rules of engagement. *Fragmentation* means that rising powers grow frustrated with the lack of, or slow pace of, accommodation from established powers and decide to create their own institutions, underpinned by their own values and interests, to compete with western-led ones. This is a scenario of more rather than less multilateralism, but of a more fragmented and less global character.[97] The BRICS Development Bank, the AIIB and the SCO can be seen as embryos of this fragmented system, which Flockhart calls a 'multi-order world'.[98] This scenario goes back to the idea of a divided world system, with multiple layers of ordering arrangements.

Some of these scenarios, particularly fragmentation, are often presented as a 'West versus the rest' case, usually opposing western hegemony and a China-led alternative. This is a slightly simplistic understanding of the complex dynamics at play, however, as there is often more overlap between these models than meet the eye, while many significant countries in the current international system sit perfectly in neither ideal-type hegemonic project. Countries such as Brazil, India or Indonesia, for example, act as bridges but are, by nature, swing states, that can support a US proposal with the same ease as they endorse an initiative coming from Beijing.

When applying Miles Kahler's three scenarios to cyberspace, we are faced with the fundamental question of whether cyber diplomacy is about the creation and maintenance of a new cyberspace order or whether its aim should be to act as a bridge-builder in a 'multi-order', fragmented cyberspace. The first option involves prioritizing stability and consensus-building over key values. The second option leads to potentially disruptive consequences in terms of cyberspace, but the potential maintenance of cyberspace's underlying liberal features, at least in (part of) the West. If we were to move towards a scenario of fragmentation, states would have to choose between increased sovereign control of cyberspace and its balkanization. As

[97] Alexander Libman and Anastassia V. Obydenkova, 'Regional international organizations as a strategy of autocracy: the Eurasian Economic Union and Russian foreign policy', *International Affairs* 94: 5, Sept. 2018, pp. 1037–58.

[98] Trine Flockhart, 'The coming multi-order world', *Contemporary Security Policy* 37: 1, March 2016, pp. 3–30.

Klimburg argues,[99] the ‘worst of the bad outcomes’ would be that liberal democracies start sleepwalking into the logic of sovereignty and information security. This is indeed what could happen if states focus excessively on bringing ‘order’ instead of something more akin to ‘managing chaos’.[100] Defining which route to take is cyber diplomacy’s greatest challenge.

[99] Klimburg, *The darkening Web*, pp. 364–5.

[100] Klimburg, *The darkening Web*, p. 317.