This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

# International Law on Cyber Security in the Age of Digital Sovereignty

https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/

ABID A. ADONIS, MAR 14 2020

Thomas Aquinas in his magnum opus *Summa Theologica* mentioned,"law is an ordinance of reason for the common good, made by those who have care of the community" (Aquinas, 1981). Unfortunately, this adage does not necessarily resonate to international law on cyberspace. The absence of effective international legal instruments on cyberspace has largely been discussed in theoretical and policy-making debates as the complexities in cyberspace render difficult for actors to come into agreements, let alone making agreeable binding law. The contentious academic debates chiefly divide those who believe that states must take more influential roles in formulating international law on cyberspace and those who insist that cyberspace should remain a free and diffused domain.[1] Beyond academic textbooks, more dynamic debates take place by stakeholders and in international institutions (World Economic Forum, 2019; Opinio Juris, 2019). All of these debates reach into one converging point: the absence of international legal regime on cyberspace is derived from actor's complexity and jurisdiction on cyber realm. This is further complicated by the fact that in the past few years several international actors, mostly state actors, promote the idea of digital sovereignty to promote their interest to take back control on information, communication, data, and infrastructure related to the internet (Gueham, 2017). Consequently, this creates harder challenges on possible future international law on cybersecurity. Hence, this puzzle requires an answer to the question I would like to address in this paper: does international law apply to states' conduct on cyberspace in the age of digital sovereignty? This article is divided into two main discussions: 1) Existing challenges on international law and governance on cyberspace, and 2) International law on cyberspace and digital sovereignty. My main argument in this article is that the binding and well-adjudicated international law on cyberspace does not effectively apply to states given challenges taken place in public international law related to jurisdiction, arbitration, and legal instruments & jurisprudences. The future of international law on cyberspace would also hardly apply to states' conduct due to the increasing trend of promotion of digital sovereignty norms.

## Existing Challenges on International Law and Governance on Cyberspace

The idea of regulating cyberspace by international law is not something remarkably novel. Since 1996, the efforts of formulating international law on cyberspace have already been continuously proposed (and refuted) by law experts, business actors, and states. There are three dominant ideas on how cyberspace should be regulated by international law: Liberal Institutionalists, Cyberlibertarian, and Statists. Liberal institutionalists like Wu (1997) call for the importance of the international institution and rule-based multilateralism in managing cyberspace. While cyberlibertarians like John Barlow (1996) are proponents of the idea that cyberspace should remain free from *tyranny* and *any oppressive rule that might hinder the internet liberty* . Statists, like James Lewis (2010), believe that it is states' responsibility to formulate national and international law to govern cyberspace. These three mainstream ideas echo into the development of international law on cyberspace. Binding and well-functioning international law on cyberspace is still absent due to these ongoing contentious debates. These debates rest on to three major challenges on formulating international law on cyberspace are related to the core of principles and characteristics of international public law: jurisdiction, arbitration, and legal Instruments & jurisprudences.

Jurisdictions in international law according to Basak Cali (2015) relates largely to the subject of international law (or actors in international relations) and territoriality to which law may be formally exercised. The subject of law or actors

in cyberspace are widely diverse and diffused as it ranges from state actors, big internet companies, small-medium enterprises (SMEs), hackers, to individuals–not to mention that internet innately also provides anonymity to its users. Those various actors also bear their own different interests and issues on how cyberspace should be regulated. It is still immensely challenging to address which subjects of law are legitimate to make and be affected by international law on cyberspace, as well as what issues should be regulated. This is also increasingly challenging to attribute conducts made by actors and where it is conducted. Numerous debates either in academic texts or policymaking have been rendered specifically discussing attribution on cyber conduct (Rid & Buchanan, 2014). Yet, there is no single dominant and prevailing voice in that debate except for those attribution of cybercrime from state actors to non-state actors in which it is relatively agreed and functioning in international regimes, such as exemplified in Interpol, Europol, ASEANAPOL, and UNODC. In terms of domain in cyberspace, international actors have not come into agreement on the status of cyberspace whether it is *global commons*, belongs to physical states' territory, or based on their national origins (Liaropoulos, 2017). As a result, it creates major challenges to determine jurisdiction of international cyber law until today.

The complexity of actors and issues discussed above render further complications in arbitration. Public international law necessitates clear dispute settlement mechanisms and arbitration to ensure that law is enacted and binding its signatories and subjects (Cali, 2015). In cyberspace law, due to its actors' diversity, there is still no universally agreed legal norm reached on who should get the mandate of dispute settlement mechanisms and arbitration. There is already arbitration on cyberspace conducts but mostly it is related to commerce and crime in which it takes place in the national legal system rather than international court (Kittichaisaree, 2017). Thus, this potentially undermines the impartiality of law since states presumably have greater bargaining power in such a legal system. Nevertheless, it is not impossible to have possible international arbitration in cyberspace. Permanent Court of Arbitration in The Hague, Netherlands might have the potential to be addressed as adjudication party on cyberspace as it already has a mandate on outer space, energy, and environmental cases. However, it needs major approval from state actors to push such mandates and authorities on cyberspace cases.

Related to arbitration, one must take into account the cyberspace challenges of legal instruments and jurisprudence. Both take place in two levels: national and international. Legal frameworks addressing cyberspace are relatively already well-developed in developed countries. In the federal level, U.S. has three fundamental regulations enacted in HIPAA (1996), Gramm-Leach-Billey Act (1999), and Homeland Security Act (2002). In France, the national authority has enacted and developed legal frameworks on cyberspace since 1988. In Russia, the federal authority also adopted the Russian Federal Law on Personal Data no. 152 FZ since 2006 (Kittichaisaree, 2017). However, those countries take a different standpoint on cyber space as Russia controversially stipulates security concern as a priority over privacy rights and the U.S. have a similar problem since Snowden's issue rise into public attention. This disparity will be widened out if we delve into cyber legal frameworks in developing countries such as Malaysia and Indonesia. Malaysia does not have a standalone cyber act or bill in which it creates room for deep state' intervention to citizen's data (ICLG, 2019). Indonesia is in worse condition–its proposed law on cybersecurity was postponed to be adopted due to massive student demonstrations in the last few months caused by human rights concerns (Jakarta Globe, 2019). These national legal framework disparities show how the absence of effective international law on cyberspace stems from national legal instruments. On the international level, the law on cybersecurity is scarce. Indeed there is Budapest Convention which is claimed to be the only international treaty on cyberspace. But one must not deny the fact that this is a lack of binding dispute settlement mechanism, tends to be state-centered, and focus profoundly on cybercrime. There is also a series of discussions on encouraging international customary law to be the foundation of international law on cyberspace (Brown & Poellet, 2012). Yet, international customary law requires reified practice and solidified legal instruments performed at the national level. As mentioned above, this is still improbable due to disparities of the national legal system on cyberspace in various countries. Efforts to formulate regulation also occur in various institutions, such as ITU, ICANN, and Internet Governance Forum in regard to governing fundamental norms, principles, and operationalities of cyberspace (Deibert & Crete-Nishihata, 2012). Unfortunately, none of those manages to overcome how international law applies effectively to states and addresses various issues in cyberspace beyond cybercrime and technicalities. None of those successfully creates appropriate and binding international legal instruments and jurisprudence. Ergo, international law on cyberspace currently is hardly effective and more difficult to be imposed on state actors.

### International Law on Cyber Space and Digital Sovereignty

The complexities and challenges of international law on cyberspace are increasingly deprived by a recent trend on digital sovereignty promotions. Digital sovereignty is the idea to control and govern access, information, communication, network, and infrastructure in digital realm by international actors (Couture & Toupin, 2019). In recent years, this idea has been gaining traction because of three historical conjunctures in cyberspace: China and Russia cyber alliance on digital sovereignty; Snowden and Wikileaks cases; and the rise of GAFA (Google-Apple-Facebook-Amazon).

China and Russia cyber alliance on digital sovereignty becomes the major precursor of digital sovereignty as both countries actively promote such an idea in order to protect their national interests which mostly are related to economy and security concerns. Both countries demand greater control of their own cyberspace by underpinning the principle of non-interference in multiple global internet governance such as ITU, ICANN, IANA, and Internet Governance Forum (Budnitsky & Jia, 2018). This sparks debate on whether the idea of digital sovereignty is against *internet neutrality* or not (Mueller, 2012). However, their efforts influentially shift the paradigm of state control over their cyberspace as that idea is supported by countries like Saudi Arabia and Egypt (Deibert & Crete-Nishihata, 2012). Their efforts also invoked the European Union to reconsider letting internet in *laissez-faire* mode continue as Snowden-Wikileaks cases rose into public attention. Security and data protection concerns have increasingly become the center of debate gravity on whether the European Union should support (Dworkin, 2015). Later, this concern has broadened up to economic consideration due to the unchecked behavior of rising big internet companies, especially GAFA. The astronomical rise of GAFA made EU consider their digital ecosystem in order to prevent business monopoly and support the innovation and internet capabilities throughout Europe (Stormshield, 2018).

These situations unequivocally set new climate of international law on cyber space in favorable to state actors. These digital sovereignty promotions and advancements would not only potentially undermine particularly non state actors and internet neutrality as the questions of freedom and liberty in cyberspace consequently emerge. These also erode the potential agreeable international law on cyber security. It is because digital sovereignty would potentially create the fragmented cyber space as it will be regulated profoundly by states on territorial basis. The idea of digital sovereignty would disconnect global internet as it is now. As a result, it hardens the possibility of international actors to come into agreement to formulate effective and binding international law on cyber space. It also hardens the possibility to adjudicate cases of cyber violations to state actors since digital sovereignty is engrained with non-interference principles–it is difficult to punish and blame state actors for their conduct in arbitration as we have seen in International Criminal Court. Alternatively, if this idea of digital sovereignty would converge state actors to come into agreement to formulate international cyber law, the law itself would be presumably dominated and determined by state actors interests with their contesting ideas of digital sovereignty at the expense of non-state actors such as business companies, individual citizens, and civil societies.

### Conclusion

The question of does international law apply to states' conduct on cyber space as discussed above denotes that the answer is not effectively. It is derived from the past and current challenges on three aspects of international law: jurisdiction, arbitration, and legal instruments & jurisprudence. In the future, the trend on increasingly promoted digital sovereignty norms potentially drive future international law on cyber space to be hardly effectively imposed on state actors. If, any, the future international law on cyber space would be nuanced by digital sovereignty at the expense of their non state actors interests. Both scenarios show that international law on cyber space is hardly effective for state actors and need broader calls for formulating rule-based, freedom-based, and inclusive global internet norms in the future.

### Bibliography:

Aquinas, Thomas. 1981. Summa Theologica. London: Christian Classics.

Barlow, John. 1996. “A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation (February 1996), http://homes.eff.org/-barlow/Declaration-Final.html. 10.

Brown, Gary & Poellet, Keira. 2012. “The Customary International Law of Cyberspace”, *Strategic Studies Quarterly*, Vol. 6 No. 3, *Cyber Special Edition*. Pp. 126-145.

Cali, Basak. 2015. *International Law for International Relations*. New York: Palgrave Macmillan.

Couture, Stephane & Toupin, Sophie. 2019. “What Does the Notion of “Sovereignty” Mean When Referring to the Digital?”, *New Media & Society*, 21(10):2305-2322.

Deibert, Ronald J. & Crete-Nishihata, Masashi. 2012. “Global Governance and the Spread of Cyberspace Controls”, *Global Governance*, 18(3): 339-361.

Duarte, Marisa Elena. 2017. *Network Sovereignty: Building the Internet across Indian Country*. Seattle: University of Washington Press.

Dworkin, Anthony. 2015. “Surveillance, Privacy, and Security: Europe’s Confused Response to Snowden”, *ECFR Policy Memo.*

Franklin, M.I. 2010. “Digital Dilemmas: Transnational Politics in the Twenty-First Century”, *The Brown Journal of World Affairs*, 16(2): 67-85.

Gueham, Farid. 2017. *Digital Sovereignty – Steps Towards a New System of Internet Governance*. Paris: Fondapol.

Jakarta Globe. 2019. *Cybersecurity Bill Postponed Until Houses Next Term.* https://jakartaglobe.id/context/cybersecurity-bill-postponed-until-houses-next-term/

ICLG. 2019. *Cybersecurity Laws and Regulations: Malaysia*. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/malaysia

Kittichaisaree, Kriangsak. 2017. *Public International Law of Cyberspace.* New York: Springer.

Lewis, James A. 2010. “Sovereignty and the Role of Government in Cyberspace”, *Brown Journal of World Affairs,* 16(2): 55-65.

Liaropoulos, Andrew. 2017. “Cyberspace Governance and State Sovereignty”, in *Democracy and an Open-Economy World Order*, ed. George Bitros & Nicholas Kyriazis. Cham: Springer.

Mueller, Milton L. 2012. “China and Global Internet Governance: A Tiger by the Tail”, in*Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, ed. Ronald Deibert, et.al., Cambridge & London: The MIT Press.

Opinio Juris. 2019. *France Declaration on International Law in Cyberspace*. https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/

Posch, Reinhard. 2006. “Digital Sovereignty and IT-Security for a Prosperous Society”, in *Informatics in the Future*. Vienna: Springer.

Rid, T. and Buchanan, B. 2014. “Attributing Cyber Attacks”, *Journal of Strategic Studies*, 38(1-2), pp.4-37.

Stormshield. 2018. *Trust: The Foundation of Europes Digital Sovereignty.* https://www.stormshield.com/trust-the-foundation-of-europes-digital-sovereignty/

World Economic Forum. 2019. *Why International Law is Failing to Keep Pace with Technology in Preventing Cyber Attacks.* https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/

Wu, Timothy. 1997. "Cyberspace Sovereignty−The Internet and the International System",*Harvard Journal of Law & Technology*, 10(3): 647-666.

**Note**

[1] Those who believe in states stronger role are including, but not limited to, Wu, 1997; Posch, 2006; and Lewis, 2010. Those who are against that argument are including, but not limited to, Franklin, 2010; Duarte, 2017; and Couture & Toupin, 2019.

*Written by: Abid A. Adonis*
*Written at: Sciences Po, France*
*Written for: Jean-Baptiste Demaison & Yann Tran*
*Date Written: November, 2019*