https://doi.org/10.48132/hdbr.307

Book Review: Cyberdiplomacy: Managing Security and Governance Online

Riordan, S. (2019) *Cyberdiplomacy: Managing Security and Governance Online*. Cambridge: Polity Press. ISBN 9781509534081

Patricia Vargas Portillo
Senior Lecturer. ESIC Business & Marketing School. Spain. ORCID: 0000-0002-0226-3053.

jennypatricia.vargas@esic.edu

Received: June, 2020.
Accepted: September, 2020.
Published: December, 2020.

Shaun Riordan, professor and former diplomat, bases the masterful work that is the subject of this review on his professional and academic experience. In this sense, as we will see below, he refers to how relevant diplomacy is for states that must face complex scenarios, such as issues related to cyberspace. In his opinion, diplomacy should be used to a greater extent in the cybernetic field. The attacks on democracy that have been provoked in the recent past should be considered in this regard. In a nonexhaustive list of such attacks, we can highlight the interference of Russia in the American elections of 2016, in which, against all odds, Donald Trump was the winner. Obviously, in this outcome, the manipulation of public opinion using the techniques of the British company Cambridge Analytica had a great impact. We could also highlight the cyberattack involving the Australian Parliament in 2018. Australia joined the United States and the United Kingdom in condemning the campaign of attacks against intellectual property and commercial data in different parts of the world, which was attributed to China. Such states referred to the group called Advanced Persistent Threat 10 (APT 10), linked to the Ministry of Security of China, as responsible for large-scale cyberaggression directed at certain service providers.

As a result of the technological developments that have been taking place with some frequency, it is necessary for diplomats to receive specific training in facing the new cybernetic scenario. Conveniently, diplomats are very attentive to any event that arises in the digital field. Thus, it should be noted that we are in a stage dominated by “fake news” and its extraordinary viralization through social networks. The term fake news became popular in 2016, when Donald Trump, president of the United States, described the news broadcast by media sources such as the New York Times and the Washington Post as fake news. From there, the concept became popular. It is true that fake news has always existed, but social networks have amplified its effects. There are

experts from various institutions working to limit the spread of fake news. For this purpose, artificial intelligence is often used. The reports of different organizations indicate that in 2022, there will be a significant amount of false news, which will make it very difficult to distinguish what is false from what is reliable. Such a situation is taking place at the present moment.

One sector of society is critical about the fact that Internet regulation has been left in the hands of technicians. Unfortunately, this has been the approach to regulation in recent years. It is likely that readers will have heard news about Huawei and 5G. Westerners sent technicians from government and industry to the important meetings at which new international standards were discussed; in contrast, the Chinese sent large diplomatic delegations. These different approaches had great relevance for both security and geopolitics. In effect, Huawei was forging the possibility of establishing a dominant position in the international standards related to the second stage of 5G. Regarding the Internet of Things (IoT), Huawei has been developing chips and software that allow companies to connect their factories to the Internet, using sensors to automate and control manufacturing lines. By the time the United States became aware of this move, too much time had passed for action to be taken. China seems to want to dominate international standards of a normative nature.

This example gives the impression that politicians and diplomats are transferring control to technicians, who should not be responsible for such issues. In reality, problems that arise in cyberspace are not technical and therefore do not require technical solutions; rather, they are problems of a political and geopolitical nature. Among them, we can highlight the regulation of the Internet, cybersecurity and cyberconflict/cyberattack.

On many occasions, as daily practice shows, the nature and type of problems that arise in the digital world reflect what is occurring in the physical world. All the handicaps that arise in cybersecurity have a notable impact on the regulation of the Internet. In all this order of issues, the loss of the global hegemony of the United States is also relevant. Likewise, diverse points of view regarding global governance are emerging. At the same time, the norms that regulate international economic and political relations are becoming fragmented. In cyberspace, these tensions are being noticed, and two large groups coexist: one in favor of free Internet and the other in favor of cyber sovereignty.

The design of international governance of the 21st century, which extends to the digital world, must consider all the changes that occur in the physical plane. Perhaps it would be advisable not to resort to intergovernmental agreements that lead to new international organizations that establish certain rules or norms (that would therefore be dictated according to a top-down approach). It would be more appropriate for new regulations of cyberspace to be developed in the opposite direction, that is, from the bottom up, through such approaches as network debates. Heterogeneous alliances or coalitions of a state and nonstate nature should be formed, such as those that gave rise to the Paris Agreements regarding climate change. Possible topics for the new normative debates that will occur in the near future are artificial intelligence, autonomous learning and genetic manipulation.

The diplomatic perspective of cyberspace is based on the concurrence of an international community in which groups comprised of members other than technicians should collaborate. In

any case, we could ask ourselves if the presence of an increasingly diverse group of nonstate actors would make the governance of the network more possible or more difficult to achieve. In the author's opinion, the difference between the physical and virtual world is increasingly tenuous. Diplomats, academics and strategists, in general, should work as if that the cybernetic world represents an extension of the physical world.

Diplomats should approach large Internet companies. However, they should not do so with commercial interest or with the aim of establishing friendly relations with their managers. They must go further. Note that these companies, which are true reference paradigms in the areas where they operate, have a significant impact on cyberspace. Although this may not seem to be the case a priori, the algorithms that these companies apply and the search engines they operate can facilitate the information war, since they provide the resources for the dissemination of erroneous information. Consequently, internet companies are geopolitical actors.

One of the purposes of the state is to safeguard its territory and citizens. With the famous attacks of September 11, the decline of the state's ability to protect its citizens from international terrorism was evident. It is well known that in this matter, only states have technological and financial means to prevent or react to attacks through protected targets or critical systems. Illegitimate actions can come not only from individuals but also from states. Awareness of countries' true intentions regarding certain issues continues to be a problem in the field of cybersecurity.

In cyberspace, it is sometimes difficult to discern an attack from a defense. The latest developments between the United States and China or Russia show that we live in a state of growing tension. Unlike the tensions that can arise on the physical plane - which can lead to the use of weapons of mass destruction - cyberwar might not be as risky. Note that there are no specific legal norms that regulate the entirety of this problem at the global level. We are facing a scenario in which governments will most likely have to modify their nineteenth-century rules of action to proceed with some speed. Similarly, diplomats will have to acquire skills in using search engines and in certain types of coding. The author masterfully describes the potential principles that must be applied in cyberdiplomacy. Among these, we can point out the necessary promotion of diplomatic qualities or attributes and adherence to current international law.

In short, the work that is the subject of this analysis brilliantly examines how the diplomatic perspective can address or manage cybersecurity, the online information war and the governance of the Internet.