DIGITAL WORLD AND REAL WORLD – OPPOSITES NO MORE

DANIEL LAMBACH

PD Dr. Daniel Lambach is a Heisenberg fellow at Goethe University Frankfurt and a senior associate fellow at the Institute for Development and Peace at the University of Duisburg-Essen. His research focuses on the construction of territory in unregulated space. His article "The Territorialization of Cyberspace" was published in the International Studies Review in 2019.

From the beginning, the internet has been spoken about as a distant place. In 2013 Germany's Chancellor Angela Merkel described it as Neuland ("undiscovered country") that was to be explored. Legal and domestic experts and policy makers like to warn the public of the "Wild West" in this ungovernable realm that exists in a "legal vacuum". Libertarian internet visionary John Perry Barlow even declared the internet's independence in 1996. Such statements are founded in the understanding of the internet as an entity of its own that is only loosely connected with the "offline world". This depiction of the internet is however quickly becoming ever more removed from the reality of the situation – if ever it was accurate. Instead, we can observe how the "digital" and the "real" world converge and infiltrate one another.

The infiltration occurs in both directions: the digital world penetrates the physical world via smartphones, optical displays, the Internet of Things and ever smaller, ever more everyday items. On the other side, the physical world penetrates the digital through techniques such as geolocation which are increasingly changing the internet's character. Geolocation is a means to establish a user's location and digitally process it. IP addresses, GPS data, transmission towers, wireless access or Bluetooth connections are all avenues via which extremely precise location information is generated – even within buildings. Anyone who has, after visiting a store, been asked to review it on Google Maps, has been the target of such technology. Geolocation can also be used for so-called "geo-blocking" when access to data and content is regulated according to one's location. Geolocation has therefore become an important tool to differentiate the marketing of intellectual property between different territories or to implement national statutes (regarding public speech, for example) via the internet.

Thus, the boundaries between the digital and the physical world are eroded,

with ambiguous results. On the one hand, it is possible to more effectively execute laws, such as when, for example, the German version of a website can be adapted to comply with German law for internet users in Germany. Economic and societal benefits include easier access to different communication channels and information sources. On the other hand, there are also dangers. For example, the potential the internet holds from being borderless can be threatened by overlaying the territorial logic of the offline world over the online world. What's more, geolocation techniques generate incredibly large, person-specific datasets which are, to this day, not sufficiently protected. In brief: we should say goodbye to the mode of thought that identifies the digital realm as separate from the "real" world. Online activities and data access will become ever more engrained in our daily social life.

The consequences will be wide-ranging for society and policy, and many of these are already playing out today. They include the removal of the boundaries between public and private spheres, between work and leisure, and the unification of online and offline identities. The adage "on the internet nobody knows you're a dog" no longer applies. States must change their classic territorially bound governing instruments to include de-territorialised ones. For example, the last few decades have seen the introduction of value-added taxes for internet trade, the sanctioning of forbidden expressions of opinion (such as holocaust denial), and debates about how to assure data protection – all without limiting the dynamics and the potential of the internet through an all-encompassing control and surveillance mechanism.

The German government has already taken action, for example, with the creation of pertinent laws ranging from specialised prosecutorial offices for internet crimes and the ability of the police to carry-out internet operations, to the establishment of the German military's Command of Cyberspace and Information Space (CIR). At the latter laws' inception, the internet was still considered to be a separate space, however this need not stand in the way of integrated action. Internet crimes are often connected with illegal actions in the physical world, and the defence against cyberattacks cannot be separated from other forms of national security.

The creation of these capacities was an indispensable step, yet how such laws and judgements are to be enforced has not yet been satisfactorily resolved. For example, how are judgements to be enforced when they are made against the users of a major internet platform such as Facebook, or perhaps even against the entire company itself? These platforms are subject to national

laws. However, the multitude of participants, or rather affected nations, can stand in the way of these laws' enforcement because of the cross-jurisdictional differences in the political and legal assessments of the crimes.

Such circumstances quickly create the impression that a national government is unable to act in the face of the new borderless realities of the digital-real world. However, this is misleading. Though traditional tactics may fail, governments still have the capacity to be creative and find new avenues of action. In fact, national governments have a multitude of options, as they can access all components that constitute digitalisation. They can regulate the technical infrastructure of cables, servers and transmission towers, for example through legal standards or access for surveillance reasons. The regulation of codes and algorithms also presents an opportunity for control. This is currently being heavily discussed in the context of Artificial Intelligence, "smart cities", and autonomous vehicles. National governments are also increasingly attempting to gain control over data by passing laws on data localisation and protection that limit the transfer and use of data. Finally, liability rules can be used to control users.

If hierarchical means such as the enforcement of laws and police powers are ineffective, national governments resort to other means. One avenue is to use their power over intermediaries that are responsible for the execution of a judicial decision. In relation to the internet, these intermediaries are more often than not large companies that are obliged to comply with court rulings by, for example, deleting justiciable comments on social media or by fighting software piracy. Another avenue is for a government to participate more in internet governance by engaging with companies, civil society organisations and experts on established rule-creating and standard-setting fora.

The final consequence of the melding of digital and real worlds concerns not only the breaking down of borders within the social spheres of societies, but also those borders between societies. Once an inseparable part of the territorial nation-state, territory is thus loosening its ties to the state a little more. Space is becoming more dynamic, movable and adaptable. We therefore have the capacity to spread our influence far beyond the borders of our currently conceived national territory. This is why the European Union's General Data Protection Regulation is followed almost world-wide. Such functional regulatory spaces reach far beyond national territories, and national governments may even be broadening their ability to exercise control.

There is a great need for such effective governance today. Many citizens feel

they are losing control due to globalisation, the dissolution of boundaries and digitalisation. Public and political discourses are marked by fears of loss and of what the future holds. It would be timely for governments to step in as the shapers of the new "digital-real world", to legitimise and uphold democracy, and to show their citizens that they do not have to fend for themselves when faced with anonymous forces in this complex new world.

There is an urgent need for further action in data protection, for example. Firstly, international cooperation in this field is still underdeveloped due to the pronounced divergence of laws in different countries. Secondly, many internet companies live off the monetisation of user data: "If you are not paying for the product, you are the product". Thirdly, more and more personal data is being accumulated and can be combined and evaluated using big data processes. Therefore, tougher rules concerning geolocation data must be developed. A ZEIT article showed how detailed personal activity profiles could be in 2009 (https://www.zeit.de/datenschutz/malte-spitz-vorratsdaten). Journalists had combined the data on Green politician Malte Spitz's movements, collected by his Telekom mobile phone, with other freely accessible data. One can imagine how this ten-year-old profile would be much more detailed today without the interference of appropriate regulation that has been implemented since that time.