ISN
ETH Zurich

30 January 2014

Cyberspace, Sovereignty and International Order

Is cyberspace beyond the reach of state sovereignty? Quite the contrary, argues Andrew Liaropoulos. He believes that it is an extension of the international system. It is a place, in other words, where national interests, geopolitical ambitions and ideologies already clash.

By Andrew N. Liaropoulos for ISN

It is now well-established that the rapid evolution of cyberspace has impacted upon almost every aspect of our lives. The dramatic increase in the speed, volumes and range of communications that it offers has undoubtedly changed the ways that individuals interact with each other, how companies deliver services and, crucially, how we are governed. But there is also a darker side to cyberspace which poses a growing number of challenges to individual and collective security.

Critical national infrastructures that depend upon computer networks have become increasingly vulnerable to cyber-attacks. The global economy is becoming ever more susceptible to cyber-crime and espionage. Yet, we are not just at the mercy of organized criminal networks, terrorist groups or tech-savvy and highly-motivated individuals. As high-profile cases such as the cyber-attacks on Estonia (2007) and Georgia (2008) – not to mention the advent of Ghostnet and Stuxnet – demonstrate, some of our armed forces might also be capable of launching hard-to-detect cyber-attacks across national borders.

So, if the cyber domain continues to provide challenges to a Westphalian state system that we have for so long taken for granted, it follows that we also need to ask a number of challenging questions. Is it possible, for example, for states to exercise their authority and control in a borderless and relatively anarchical 'cyber' world? Paraphrasing Hedley Bull's concept of international order, one could argue that exercising state sovereignty in cyberspace is a necessary step for establishing an international cyber-order. According to Bull, states act in such a way as to preserve international order, because this order is in their own interest. An additional question to be asked then is whether states will act in the same way in cyberspace in order to preserve an international cyber-order.

Debunking a Myth

Irrespective of all the changes that continue to shape our world, sovereignty remains an important and fundamental concept for the current international order. Sovereignty not only signifies authority within a distinct territorial entity, it also implies membership of the modern states system. Yet, defining what actually constitutes sovereignty in international politics remains a challenge. A useful

typology of sovereignty is provided by Stephen Krasner, who identifies four ways in which it can be understood: domestic sovereignty, interdependence sovereignty, international legal sovereignty and, of course, Westphalian sovereignty.

Domestic sovereignty refers to the way public authority is organized within a state and to the level of effective control that these authorities can exercise. Political systems of all shapes and sizes are responsible for regulating and controlling developments within their own territory. By contrast, interdependence sovereignty relates to the ability of public authorities to control trans-border movements such as flows of people, materials and ideas across borders. If a state fails to regulate what passes across its borders, it will also fail to control what happens within its territory. Accordingly, the loss of interdependence sovereignty has the potential to impact upon domestic sovereignty. International legal sovereignty sees things a little differently, given that it is particularly concerned with the mutual recognition of states in the international system. Finally, Westphalian sovereignty highlights the right that states have to determine their government and politics free from the influence of external actors.

David Betz and Tim Stevens use this typology to debunk the myth that cyberspace is immune from state sovereignty. In their book *Cyberspace and the State: toward a Strategy for Cyber-power*, they argue that this myth is based upon a widely-held belief that cyberspace *is not a physical place* comparable to land, sea, air and outer space. But while actions in the cyber domain seem to take place *outside* the state in a *virtual* manner, their effects nevertheless have *real* world implications that are quite often felt *inside* states. This is because cyberspace requires a physical infrastructure in order to operate. And such infrastructure is terrestrially based and therefore not immune from state sovereignty.

Betz and Stevens further argue that cyberspace cannot operate in a chaotic manner and instead requires regulation and oversight. Companies that operate in cyberspace need the laws of state to operate their business. Finally, states need to be present in cyberspace and exercise control for reasons of national security. Preventing a repeat of the Stuxnet episode, for example, is likely to be high on Iranian policymakers' and security practitioners' agendas. National critical infrastructures such as oil and gas pipelines, electricity and water supplies and transportation networks all rely upon computer networks to operate. Consequently, they should not be beyond the purview of the state.

However, state-based oversight of the cyber domain also comes with its fair share of problems. Efforts to control cyberspace in both authoritarian regimes and liberal democracies has often resulted in denying citizens access to information on the basis that it may compromise national security and sovereignty. This might entail the removal of politically-charged videos from websites, restricted access to social media channels, filtering surveillance techniques and other devices that limit anonymity in cyberspace.

The Challenges Ahead

Consequently, states have to overcome a number of technical and political challenges if they want to safeguard sovereignty *and* promote order in cyberspace. As comparatively recent cyber-attacks on government websites and industries suggest, attributing these to specific actors is always going to be problematic, at least for those states that lack the wherewithal to fully investigate such incursions. Creating an international investigative body, based on the International Atomic Energy Agency (IAEA), to review and investigate cyber-attacks, might not answer the attribution problem, but it might be a step in the right direction.

This, in turn, reflects that reaching a consensus on the proper use and regulation of cyberspace is

another major challenge that needs to be addressed. The ‘great cyber-powers’ – China, Russia and the United States – will undoubtedly be at the forefront of such an initiative. However, all three have contrasting views on how best to govern the cyber domain. For example, Beijing and Moscow do not share the US position that existing international laws should apply to cyberspace. In September 2011, both countries submitted their proposal for a code of conduct in cyberspace to the United Nations General Assembly. The proposed code calls upon states to respect domestic laws and sovereignty and settle disputes within the framework of the United Nations.

There’s also the issue of *how* these states use cyberspace to play great power politics. It may be the case that China opposes Washington’s proposed initiatives to govern the cyber domain because it views its cyber-warfare capabilities as powerful asymmetric tool to deter the United States. In this respect, it also seems quite plausible that Moscow views cyberspace through similar lenses to Beijing’s. For its part, Washington continues to emphasize the very real danger of cyber-attacks by state and non-state actors to justify the development of offensive cyber capabilities that not only defend US interests, but also those of its allies.

Accordingly, cyberspace provides a number of challenges to sovereignty that states simply cannot afford to ignore. The cyber domain is a reflection of the current international system, where national interests, geopolitical ambitions and ideologies will inevitably clash. But it’s also where states will choose to cooperate with one another with a view to safeguarding international order and security.

We still have a long way to go before states reach a consensus on the appropriate use of cyberspace in international relations and security. Then there’s the small matter of developing effective mechanisms for oversight and control. Yet it is fair to say that efforts to develop an international cyber-order are already underway. As a result, Bull’s seminal work on international order might serve as a useful guide for investigating the behavior of states in cyberspace over the coming decades.

Andrew N. Liaropoulos is a Lecturer in the Department of International and European Studies, University of Piraeus, Greece.

Publisher

International Relations and Security Network (ISN)

---

http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=176144&lng=en

---