Cyber Diplomacy with Africa: Lessons From the African Cybersecurity Convention

Blog Post *by* Guest Blogger for Adam Segal

July 7, 2016

CFR Cyber Net Politics

*Mailyn Fidler is a Marshall Scholar studying international relations at the University of Oxford. You can follow her on Twitter **@mailynfidler**.*

Two years ago, the African Union (AU) adopted its Convention on Cybersecurity and Personal Data Protection. The Convention seeks to improve how African states address cybercrime, data protection, e-commerce, and cybersecurity. However, only eight of the AU's fifty-four members have signed the Convention, with none ratifying it. Despite this currently limited uptake, the Convention, and how the AU produced it, signals that African states value political autonomy and independence when developing cyber policy. The U.S. government should keep this in mind as it reaches out to AU member states in promoting cyber norms and capacity building

THIS SITE USES COOKIES TO IMPROVE YOUR USER EXPERIENCE. CLICK
HERE TO LEARN MORE.

Close

The AU's development of the Convention reflects a desire of African states to have autonomy over their response to cyberspace challenges. The AU chose to develop its own Convention instead of promoting African participation in existing cyber treaties, most notably the Council of Europe's Budapest Convention on Cybercrime (2001). Only one African state, South Africa, participated in the Budapest Convention negotiations, and, even then, had to ask to be included. The Council of Europe approved three other African country requests to accede, a low rate compared to other regions in the global south, and only one African state has ratified it. South Africa has refused to ratify the Budapest Convention because of sovereignty concerns.

Instead, the AU began work on its own approach in 2007. By this time, African states had already started to act as a bloc in international cyber negotiations. For instance, African countries advocated for more equitable access to the Internet and participation in Internet governance during the 2003 and 2005 World Summit on the Information Society (WSIS) – a stance that challenged prevailing Western views. African solidarity against perceived Western dominance was not limited to cyber issues. At the time, African states were negotiating new Economic Partnership Agreements with the European Union, with African governments resisting clauses they perceived as unequal and patronizingly conditional. Some governments also expressed discontent that the International Criminal Court was unfairly targeting African leaders.

In 2006, the Economic Community of West African States (ECOWAS) began promoting harmonization of data protection, e-commerce and cybersecurity legislation among its members. ECOWAS received support from the International Telecommunications Union and the European Commission for this work as part of the WSIS outcomes. These efforts, and those of other African regional organizations, provided the catalyst for the AU Commission to

THIS SITE USES COOKIES TO IMPROVE YOUR USER EXPERIENCE. CLICK HERE TO LEARN MORE.

Close

Interestingly, influential African states, such as South Africa, Kenya, and Nigeria, played little role in the Convention's development, which was instead spearheaded by African Union officials and bureaucratic partners in select African regional organizations. For example, the AU consulted ECOWAS officials about the Convention's development, but the Nigerian government played little role. The Convention also lacked support from civil society groups and some international companies because of its questionable human rights clauses.

Instead of support from regional powerhouses, the Convention has attracted endorsements from less powerful states. Benin and Guinea Bissau signed the AU Convention first (January 2015), followed by Mauritania (February 2015), the Republic of Congo (June 2015), and Chad (June 2015). These signatories are Francophone, reflecting the Convention's substantial West African roots. In January 2016, Zambia, Sierra Leone, and São Tomé and Príncipe signed, representing the first signatories without significant Francophone influence. No state has ratified the Convention, which requires 15 ratifications to enter into force.

Although the content of the Convention mirrors that of the Budapest Convention, European approaches to data protection, and other Western ideas on cybersecurity, the Convention's politics emphasize an African desire for independence, particularly from Europe. The AU did not invite the Council of Europe to provide formal feedback on the treaty. In contrast, the AU requested and lauded U.S. input. These decisions reflect the AU's desire to establish greater autonomy in African approaches to cyber policy, especially from the countries that have historically dominated it: a cyber version of "African solutions for African problems."

Challenges for U.S. Outreach

The United States needs to keep this African desire for autonomy and independence in mind as

Washington will want to stave off closer cooperation between African countries and China. The AU, for example, recently announced a program to work with the China Cyberspace Administration, but the details of this cooperation, including whether it involves mainly investment or cooperation on legal approaches, remain sketchy. The challenge for the United States will be to remain Africa's cyber partner of choice without becoming overbearing, insisting that it has the only right approach to cyber problems, as it does with other issues. It can form an effective partnership only by recognizing the AU's autonomy and independence.