

Africa Endeavor 2019
As Prepared
Opening Remarks by U.S. Chargé d'Affaires Christopher J. Lamora
Mövenpick Ambassador Hotel Accra
19 August 2019

Honorable Minister of National Security, Albert Kan-Dapaah
Hon. Minister of Defense of the Republic of Ghana, Dominic Nitiwul
Hon. Minister of Communications of the Republic of Ghana, Ursula Owusu-Ekuful
Hon. Chief of Defense Staff of the Ghana Armed Forces, Lt. General Obed Akwah
Hon. Chief of Staff of U.S. Africa Command, Major General Todd McCaffrey
Honorable Service Chiefs of the Ghana Armed Forces
Distinguished Guests and Visitors,

I'm delighted to be here this morning, together with so many civilian and military security professionals from more than 40 countries, who have gathered in Ghana to discuss our shared, mutual interests in the broad field of military communications.

United States Africa Command (or AFRICOM) and the Ghana Armed Forces have gone to great lengths to assemble world-class speakers and participants, each of whom brings a wealth of knowledge and expertise from their home countries. It is therefore particularly appropriate, as you discuss communications interoperability, that you give and take the best ideas everyone in the room has to offer.

This conference will cover quite a number of topics, including two that are of particular importance for the United States and Ghana.

The first is the crucial role of women in advancing and solidifying international peace and security... a topic that is particularly appropriate as we celebrate the 60th anniversary of women serving in the Ghana Armed Forces. We often talk about the importance of fostering women's political engagement and economic empowerment, and certainly those are critical underpinnings for the future success and development of any society. But women who serve in, or oversee, their countries' security services play a uniquely important role. During yesterday's "Women's Signal Forum," 27 women from 26 countries deliberated and shared best practices on creating gender balance in peace and security decision-making. We recognize Ghana's leadership in this area, and I encourage all of you to keep this critical conversation going well after you have returned home.

The second topic that is very much in line with U.S. priorities – not just in Ghana, but globally – is cybersecurity, including our common objective of an open, interoperable, secure, and reliable cyberspace. Here in Ghana, we collaborate closely with the government, through the Security Governance Initiative, to promote best practices in cyber security... both the security of cyber platforms themselves, and mitigating the possibility that cyberspace could be exploited for criminal or other nefarious purposes.

I know that we have with us in the room today a number of leaders in this field who are well-positioned to advance our global efforts to promote cybersecurity best practices. Alongside those experts are undoubtedly others (such as myself) who may not be expert in these technologies but who are nonetheless dedicated to striking the right balance between a fully accessible Internet that facilitates information-sharing, trade and commerce, and one that includes protections to mitigate against dangerous vulnerabilities and threats.

Every technological advancement in history has presented new opportunities and challenges, and the Internet is no exception. Cyber-enabled threats have proliferated as our systems have become more and more interconnected. These threats range from state-sponsored attempts to target major critical infrastructure to the use of ransomware by cybercriminals to extort a single individual or hold hostage sensitive information.

So how do we deal with these growing threats to our networks and infrastructure?

Addressing this question will be a key part of what you discuss over the coming days. What best practices have some countries or security services adopted that might be applicable somewhere else? How can National Cyber Strategies and whole-of-government approaches increase awareness, education and training? What opportunities might exist for public-private partnerships? How do we most effectively share information across borders to ensure that no country becomes a safe haven for malicious cyber activity?

You may not find the answers to all of these questions in the coming days, and of course there's no "one size fits all" solution. National Cyber Strategies must be tailored to each nation's own realities, aspirations, and goals. But in developing those strategies, all governments benefit from seeking input from the private sector and civil society. This includes educating citizens and industry representatives about their own important roles in protecting cyber systems. We must foster cybersecurity talent, as a highly-skilled cadre of cybersecurity experts is a strategic

national security advantage. And we should listen to, and learn from, each other on how best to develop this expertise. Only by taking this sort of methodical approach will we be able to articulate our objectives, define our priorities, and allocate resources to address our respective nations' cyber concerns.

The work of each of you in this room, and the organizations you represent, is fundamental to this effort. Our relationships and partnerships are key to mitigating threats and defending our countries and citizens against cyber threats.

I hope that this conference will create space for open and fruitful conversation. As you move forward in your work, know you can count on the continued support of the United States. Thank you.