STRENGTH
IN NUMBERS

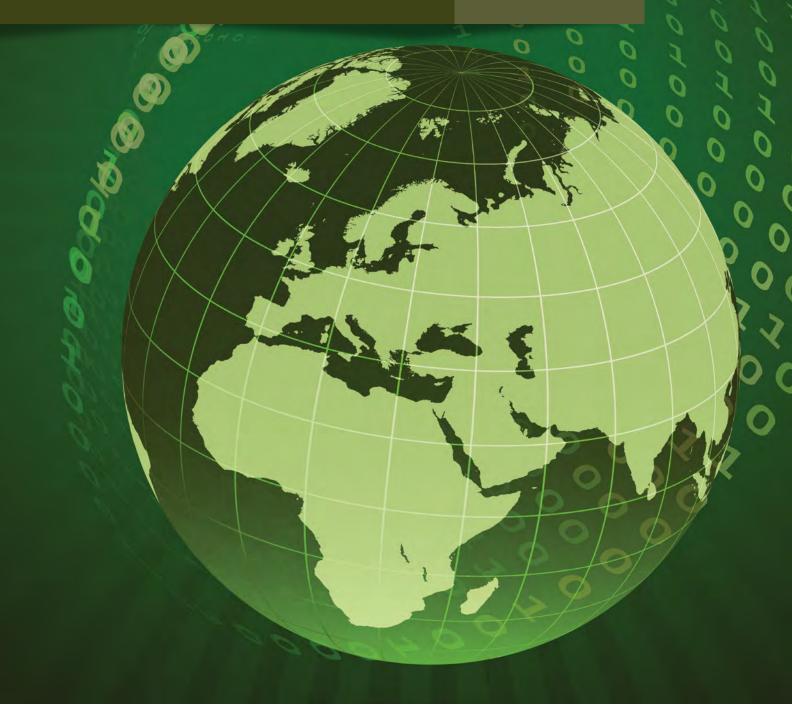**PERSPECTIVES ON THE AFRICA ENDEAVOR 2017 SYMPOSIUM**

By *Capt. Domingos Tavares,* Armed Forces of Cape Verde

Internet and mobile technologies permeate Africa, transforming all aspects of human life on the continent and inducing a transference of humanity to cyberspace. The challenges of digitalization are apparent as cyber crime meets a deficit of cyber security laws, and combatting traditional crimes requires transnational interoperability. Africa Endeavor 2017, held in Malawi, underscored some significant cyber security shortfalls that most of the continent has yet to consider. Senior representatives of many African nations attend the annual symposium co-hosted by U.S. Africa Command and an African partner country.

The presentations generated strong audience engagement and a tremendous interest in comprehending not only the parameters of cyber security, but how to begin addressing the problems. It is this author's view that countries such as Cape Verde that have already begun to address cyber security issues must be available to help others by becoming partners in the fight against cyber crime. But the most important step is to convince policymakers of the importance of cyber security and the need to create laws that, if compatible with international partners, can effectively address cyber crime.

During Africa Endeavor, representatives from the Netherlands effectively illustrated that cyber security often begins with the user, whose ignorance or carelessness can expose all manner of personal data on digital platforms. The presentation emphasized the importance of being alert when using certain websites and the importance of having a strong and secure password.

The conference also addressed the nature of transnational organized crime, which now has a cyber security component. Nations must contemplate the many consequences associated with maritime piracy, illegal fishing, and the trafficking of people, animals and goods. The communication and cooperation encouraged at Africa Endeavor, where the objective is to analyze and overcome interoperability challenges, can play a fundamental role in solving these challenges.

In 2016, Cape Verde approved the National Strategy for Cybersecurity, making clear that it is key to the country's development. The strategy's primary objective is to protect the country from cyber threats and crimes by assigning responsibilities to national, international and global actors.

Cyber security is key to development because the country is heavily dependent on communication technologies, and its vulnerabilities are increasing as a result of this dependency. We have an electronic governance structure, a high

Clients browse the internet at a cyber cafe in Mogadishu, Somalia, in 2017. With the African population becoming ever more connected, the need for cyber security is essential.

Taiwanese and Chinese nationals arrested on suspicion of telecommunications fraud listen to a translator in Nairobi, Kenya. Cyber fraud is a growing concern as Africa expands its digital footprint.

saturation of internet subscribers (about 70 percent of the population), and a society that intertwines personal and business communications.

The strategy addresses the issue of cyber security for citizens and for public and private institutions. It sends a strong message that we will not allow Cape Verde to become a paradise for cyber criminals drawn to countries where there are no legal consequences for cyber crime.

The country has been working toward international cooperation with the African Union and the Economic Community of West African States, with the support of partners such as the United States. A major objective is to create a national cyber security center that will include a computer emergency response team that should serve in all sectors, including national defense.

Cyberspace is an open world in which the crime and the criminal are not necessarily located in the same place. The targets may be civilian, military or paramilitary infrastructures, and a decreasing distinction between these factors is becoming more evident. Therefore, it is essential that the military is capable of dealing with cyber threats that jeopardize security, and it is also essential that there be information sharing with the civilized world because cooperation in the digital domain is essential.

Africa Endeavor 2017 provided a forum for addressing national and regional security concerns on the African continent, and it remains a solid foundation upon which to build further integration and interoperability capabilities to address internet-based threats, cyber security shortfalls and the continually changing nature of today's criminal activities. □