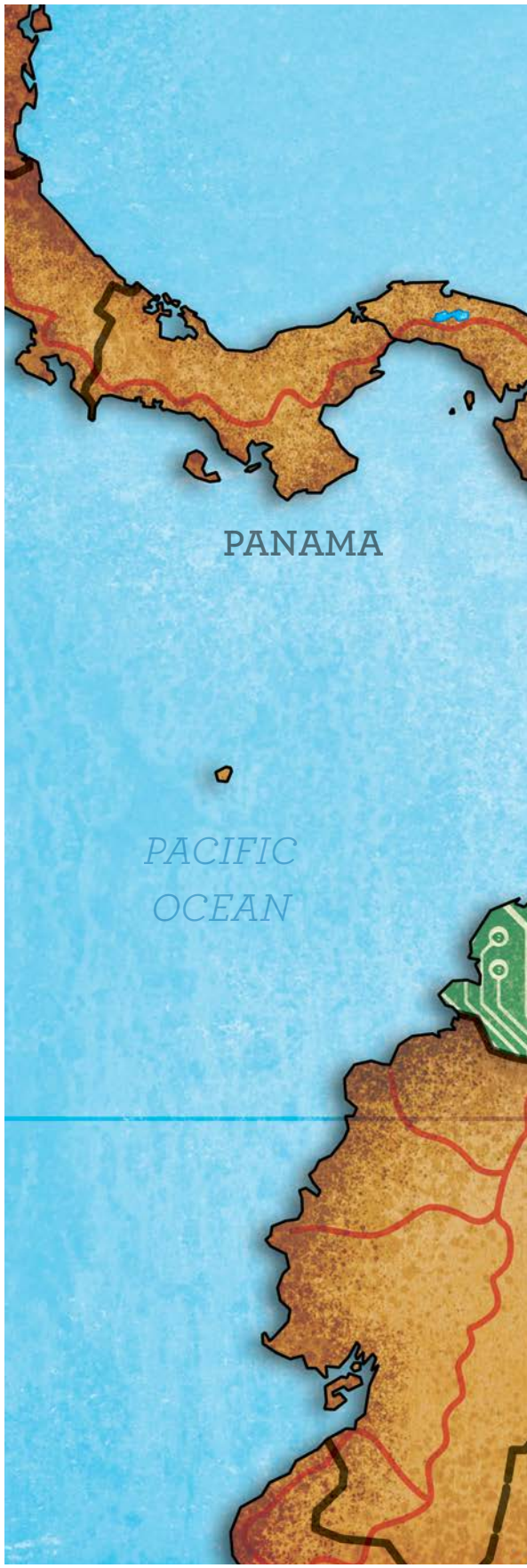
CYBER SECURITY *in* SOUTH AMERICA

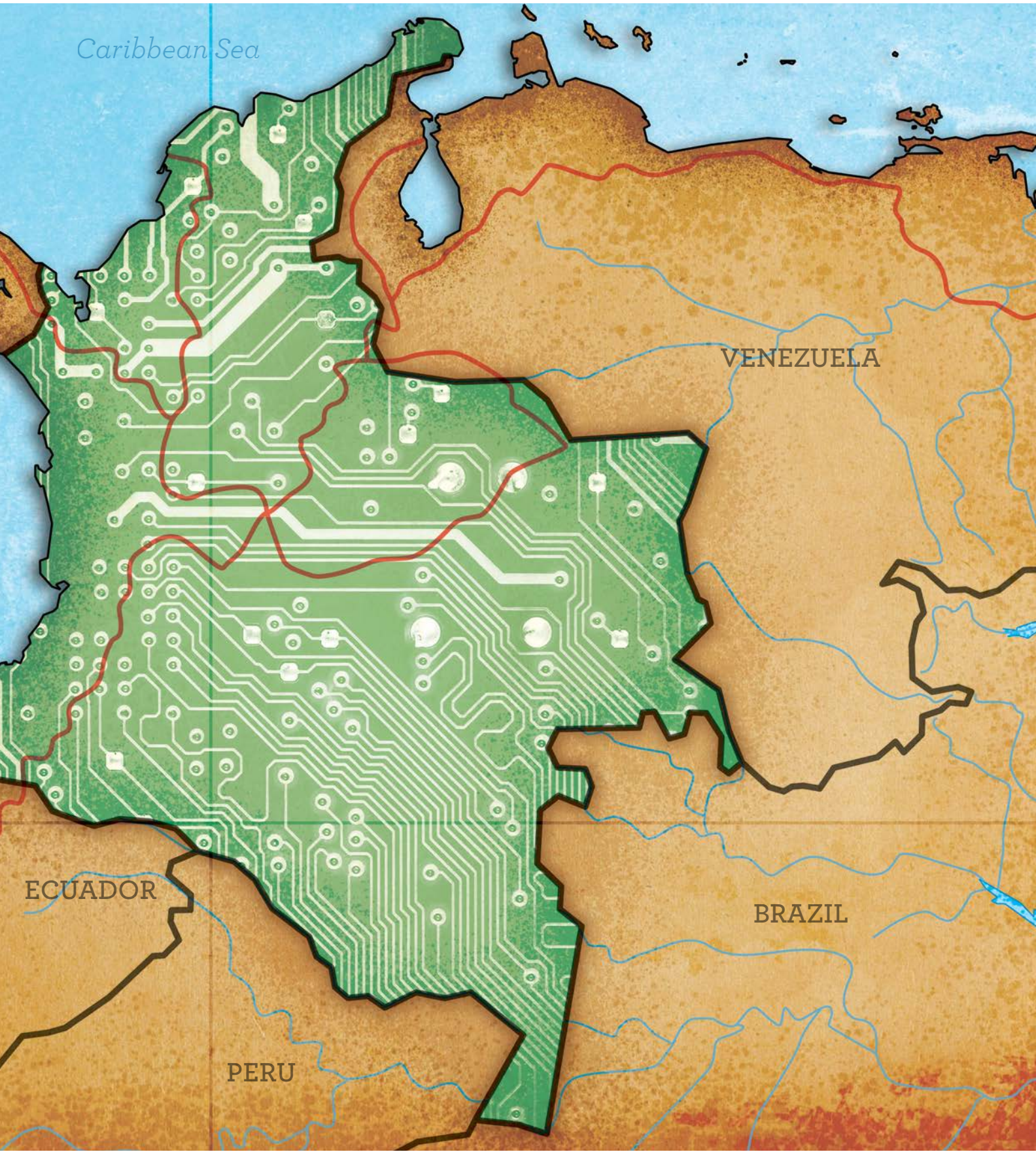
Colombia develops a comprehensive new cyber security policy

By **Alvaro José Chaves Guzmán**,
Ministry of National Defense, Colombia

The digital economy and Internet culture are spreading through the developing world at an increasingly rapid pace, and Colombia is leading the way. According to the *Affordability Report 2014*, published by the Alliance for Affordable Internet, Colombia ranked second among 51 emerging economies in Internet connectivity. The honorable second place ranking was due, the report concludes, to a series of efforts made by public and private entities to heavily invest in infrastructure in rural parts of the country, and a concerted effort to increase literacy in information and communications technology (ICT) issues. These two efforts helped the country provide access to the Internet to more than half the population.

Colombia's effort boosted Internet users significantly — from 2.2 million Internet connections in 2010 to over 9.2 million in 2014. In this regard, Colombia became the first country in Latin America with high-speed Internet coverage for all of its municipalities.





PER CONCORDIAM ILLUSTRATION

However, in recent years, the Internet has been increasingly used for criminal purposes. Since 2007, Colombia has been building a national strategy to combat cyber crime, focusing on cyber defense and cyber security. The strategy rests on three pillars:

- Pillar 1: Adopt appropriate institutional framework to monitor threats and prevent attacks, coordinate responses, and generate recommendations to address threats and risks in cyberspace.
- Pillar 2: Train personnel in information security and expand research on cyber defense and cyber security.
- Pillar 3: Strengthen legislation, international cooperation and advance adherence to international instruments to fight cyber crime.

To develop these strategies, Colombia designed and implemented four entities:

- Intersectoral Commission: Sets the strategic vision of information management and policy guidelines for technological infrastructure, public information, and cyber security and cyber defense.
- Colombia Computer Readiness Team (colCERT): Coordinates national aspects of cyber defense and cyber security.
- Joint Cyber Command General Command of the Armed Forces: Defends against cyber threats, in particular it protects national critical infrastructure and the defense sector.
- Police Cyber Center: Supports and protects through the Comprehensive Strategy against cyber crime.

The planned strategy meets three goals:

- Improves coverage and technical capabilities by creating specialized units.
- Pairs and ensures the active participation of stakeholders in the strategy through a stewardship thereof, articulates the strategy to the private sector, strengthens citizen education and improves all levels of prevention through social networks and other channels.
- Disrupts criminal structures through comprehensive crime analyses, investigates and impedes the cyber crime economy by linking the national police to different international scenarios, all aligned with the national policy document that defines the guidelines of cyber security and defense.

> Undoubtedly, the objectives of economic and social prosperity in Colombia are fundamental, and overcoming the challenge of securing and defending the nation's cyberspace is important to achieve these objectives.

Colombia's national cyber crime strategy was implemented through the Ministry of National Defense. While these efforts acknowledge the importance of the subject internationally, it is important that the national government strengthen its leadership and build a new, clear overview for an integrated approach that recognizes international best practices for addressing the risks in cyberspace.

Internet access has increased dramatically in Colombia, emphasizing the importance of good cyber security. AFP/GETTY IMAGES

Today, advances in digital networking require the establishment of a safe and secure digital environment throughout society. Even though institutions and agencies created by the Ministry of National Defense have been tasked with the responsibility to defend against and respond to cyber attacks and cyber crime, it is necessary to integrate more coherent actors in the national government, private organizations and civil society to reduce the risks of dangerous behavior or lack of information regarding necessary security measures.

This new policy document seeks to update cyber defense and cyber security goals and articulate the capacities created thus far. Its development has been supported by high levels of government with efficient and comprehensive involvement in all institutional models by each of the interested actors; namely the national government, public and private organizations and civil society. The policy objectives of the document are economic and social prosperity in the country with the goals of establishing a capable cyber defense, fighting cyber crime in the digital environment and implementing a set of fundamental principles that advance specific actions under the strategic risk management of digital security dimensions.

Undoubtedly, the objectives of economic and social prosperity in Colombia are fundamental, and overcoming the challenge of securing and defending the nation's cyberspace is important to achieve these objectives. That is why the new cyber policy document should become the foundation of a national strategy that will bring Colombia's cyber capabilities to a new level. By properly recognizing constitutional rights and freedoms in the virtual world, with a focus on risk management, the protection and defense of cyber critical infrastructure and national interests in cyberspace, protection of personal data and privacy for citizens, we can create an environment that contributes effectively to the economic and social prosperity of the country. □