BACKGROUND AND CONCEPT

The Security Institute for Governance and Leadership in Africa (SIGLA), Stellenbosch University, and the U.S. Defense Threat Reduction Agency (DTRA), International Counterproliferation Program (ICP) have been in partnership since 2016.

SIGLA has a strong focus on building leadership capacity and knowledge in security for sustainable development in Africa. The Institute's research program spans security and governance issues across the terrestrial, maritime, and cyber domains. This includes Africa's digital space, cyber threats and emerging technologies. SIGLA Cyber was launched in 2018 with a special emphasis on cyber warfare and cyber strategy and their role in terms of development within the military and security context. It has since grown in its scope and activity to include systemic and societal cyber threats. SIGLA Cyber's emphasis is on creating and giving effect to innovative partnerships across academia, industry, and government within Africa which aim to strengthen digital security competencies, deepen research and promote resilience.

ICP is a congressionally mandated program led by the U.S. Department of Defense, in conjunction with the Federal Bureau of Investigation and the Department of Homeland Security. The ICP mission is to employ a whole-of-government approach to build measurable and sustained partner nation capacity to prevent, detect and counter weapons of mass destruction (WMD) proliferation threat networks.

The partnership between SIGLA and ICP has resulted in a series of International Workshops on Combating Transnational Crime in Africa. The inaugural event in 2017 addressed threats and vulnerabilities in the maritime domain, and the 2019 event focused on Border Management and Security – both bringing together an amalgam of policy makers, academia and practitioners.

Following the pause driven by the COVID pandemic, the collaboration is set to continue, in March 2023, with a third workshop in the series. The focus is on countering cyber threat proliferation, based on the following broad rational:

"Today's globally interconnected world presents a wide array of serious risks and threats to critical infrastructure, systems, assets, functions, and citizens. Given the dynamic threat landscape and significant developments in global cybersecurity and related policies, the international community must remain fully engaged to shape an environment that will preserve national and economic security interests.

Strong partnerships strengthen a nation's ability to globally defend against cyber incidents, enhance the security and resilience of critical infrastructure, identify and address the most significant risks to the national critical functions, and provide seamless and secure emergency communications. Sharing threat information, mitigation advice, and best practices with international partners not only reinforce good cyber hygiene, but also bolsters the resiliency within our respective systems and critical infrastructure, which in turn, foster a safer cyber-physical ecosystem for all."

The workshop will once again bring together experts and practitioners from the international and African regional communities. Keynote speakers will set the tone for sessions and moderated panels will address a developed range of topics, culminating in an interactive discussion focused on moving from policy into action.