



**Permanent Mission of Saint Vincent and the Grenadines
to the United Nations**

685 3rd Ave., Suite 1108, New York, NY 10017 • Tel: (212) 599-0950 • Fax: (212) 599-1020 •

svgmission@gmail.com | <http://svg-un.org>

Statement

by

H.E. Dr. Halimah DeShong

Deputy Permanent Representative of Saint Vincent and the Grenadines
to the United Nations

**Arria-formula meeting of the Security Council on Cyber Stability, Conflict Prevention
and Capacity Building**

United Nations Security Council
22 May 2020
New York

Mr. President,

I wish to thank His Excellency Mr. Jüri Ratas, Prime Minister of the Republic of Estonia for his opening statement, as well as today's briefers for their comprehensive presentations. We also thank Estonia and co-hosts Belgium, Dominican Republic, Indonesia and Kenya for organizing this meeting.

As we move further into the 21st Century, one thing is certain, no country's government or population is immune to emerging cyber threats. This is especially true in the developing world, where glaring cyber-capacity shortfalls exist, allowing rogue actors to prey on the most vulnerable amongst us in cyber-space. Despite our many challenges, Saint Vincent and the Grenadines adopted its Cybercrime Act in 2016, which creates a legal framework to address offences related to cybercrimes.

Yet, when faced with the borderless realities of cyber-space, we acknowledge that no country or region can go it alone. Saint Vincent and the Grenadines emphasizes that confidence building measures and information exchange amongst member states and regional organizations are essential for ensuring stability in cyberspace and to prevent escalations of cybersecurity incidents. We therefore encourage initiatives that facilitate this strategic coordination at national, regional and global levels. These efforts must also include non-state actors from the private sector, civil society, academia, and should entail workshops and capacity-building exercises to manage and prevent disruptive cybersecurity incidents.

As a matter of urgency, the rise of surveillance capitalism as a primary feature of today's technosphere necessitates data governance models that protect the privacy of citizens and safeguards the integrity of democratic electoral processes. In cyberspace, we encourage all actors in the international community to comply with their international legal obligations including the respect of sovereignty and political independence as enshrined in the UN Charter, and the principles for peaceful dispute settlement in the same manner as in the physical world.

To conclude, failure to agree on the rules of engagement, policy norms, and international cooperation mechanisms for cyberspace would only yield new sources of instability and conflict. But before we can even achieve this international cooperation, a level playing field must be created whereby each state is empowered to exercise sovereign control over its own cyberspace. Only then can the internet of things form part of our global commons. And only then can we achieve the collective action required to enjoy peace in the digital age.

Thank you.