United States remarks for March 2022 session of the OEWG, as prepared

On CBMs

- Voluntary CBMs can increase international cyber stability. Through transparency measures, CBMs can create more predictability about state activities in cyberspace. Through cooperative and communication measures, CBMs can help states manage escalation in the event of a serious cyber incident. CBMs are an essential element of the framework for responsible state behavior in cyberspace.

- The 2015 GGE report offers a prioritized set of cyber CBMs, including recommendations to develop points of contact, consultation mechanisms, and transparency measures. The 2021 GGE and OEWG reports also provide robust recommendations on CBMs.

- To be useful, however, these recommendations must be implemented. The OEWG should review the CBMs identified in the 2015 GGE report and provide additional guidance, as necessary, to assist States in this implementation. This OEWG should also identify emerging best practices in cyber CBMs gleaned from the extensive work on CBMs undertaken in certain regional bodies.

- The United States is a member of three regional organizations with cyber CBMs programs: OAS, OSCE, and ARF. Each organization is different, but some elements of success cut across the regions.
  - Consistency is key
• CBMs take months if not years to become operational. Because of that, CBMs programs benefit tremendously from self-reinforcing arrangements. The ARF created a dedicated regional venue on cyber CBMs within the organization, which established leads, regularized discussion, and clarified reporting structures. OAS established a more permanent secretariat with the responsibility of managing the cyber CBMs group and its projects. OSCE developed an “adopt a CBM” program, where individual member states take responsibility for putting a CBM into action. These arrangements help CBMs programs maintain momentum.

  o CBMs should be exercised

  • One specific activity that moves CBMs from conceptual to functional is the exercise or testing out of a specific measure. This is particularly helpful for measures intended to be used in the event of a significant cyber incident, such as POCs directories. Such exercises can consist of a simple confirmation that POC information is up-to-date and functional or more elaborate exercises that simulate a damaging cyber incident that affects the region where CBM measures could play a mitigating role.

  • The United States continues to believe that cyber confidence building measures are best implemented by regional organizations with the capacity and regional expertise to take on such programs and adapt them to their regional context. The United Nations’ primary role on cyber CBMs should be to develop
global recommendations, share best practices, and encourage cross-regional dialogue and exchanges when appropriate.

- Only half the world has pursued a regional cyber CBMs framework at this point. Not all UN member states are members of multilateral or regional organizations with cyber CBMs programs. We believe the UN should support cross-regional information sharing on cyber CBMs. We believe that such information sharing can be valuable, but there are limits to that value — replicating what works in one region will not ensure success in another region, so there must be regional adaptation and ownership.

- We support the OEWG’s work on CBMs but want to ensure that such efforts do not distract from or undermine ongoing activities in regional organizations. We must also be realistic about the UN’s capacity to take on a larger role on cyber CBMs. Despite those concerns, we believe the OEWG can make substantial contributions to international adoption of cyber CBMs programs.