ورقة مصرية مقدمة إلى

فريق الخبراء الحكوميين التابع للأمم المتحدة حول موضوعات الأمن الدولي للمعلومات

بين الجولتين الثانية والثالثة لاجتماعات الفريق

فبراير 2015

سامح أبو العينين (مصر)

---

1. **يحق لحكومات الدول اتخاذ التدابير والسياسات اللازمة المتعلقة بتكنولوجيا الاتصالات والمعلومات طبقا لمتطلبات الأمن القومي لكل دولة.**
2. **أهمية التعاون الدولي وتعزيز تدابير بناء الثقة بين الدول بما يكفل الإنذار المبكر لأي تهديدات عدائية قائمة أو محتملة تتم من خلال (أفراد/ جماعات/ دول) وكذا تبادل الخبرات في مجال الأمن السيبراني.**
3. **ضرورة قيام كل دولة على حدة بتشريع داخلي من خلال القانون الجنائي لها للجرائم المعلوماتية وتوصيفها وكذا وضع عقوبات رادعة لمرتكبي هذه الجرائم.**
4. **الاتفاق على آليات ومصطلحات وبنود ثابتة لكافة القضايا الخاصة بالفضاء السيبراني (البنية التحتية الحيوية – الجرائم الإلكترونية – ...) لمتابعة الحوادث الإلكترونية حيث أن الاختراقات والتهديدات والجرائم السيبرانية تعد من أعمال الحرب غير التقليدية.**
5. **التركيز على أسلوب المجابهة للتصدي لمخاطر تكنولوجيا الاتصالات والمعلومات والوقاية منها بشكل مسبق وذلك قبل وقوع الأزمة.**

Egyptian Inter-session Input Paper

for the Work of the

Group of Governmental Experts (GGE)

February 2015

Sameh Aboul-Enein (Egypt)

-----

1. Each government is entitled to take the necessary measures and policies relating to communications and information technology, according to the requirements of the national security of each State.

2. The importance of international cooperation and the promotion of confidence-building among States in order to ensure early warning of any potential or current hostile threats from (individuals / groups / nations), as well as the exchange of experiences in the field of cyber security.

3. It is necessary that each State develops an internal legislation system through its criminal law for relevant cyber crimes, as well as the development of deterrent penalties for perpetrators of such crimes.

4. The agreement on constant terms, mechanisms and items for all the special issues of cyber space (critical infrastructure - Cybercrime – etc.) to follow the cyber attacks, as the cyber intrusions, threats and crimes are acts of unconventional warfare.

5. Focusing on the confrontation mnechanism against all the relevant risks of communication technology, information, and the pre-crisis prevention measures.