الجمعية العامة الـ 145 للاتحاد البرلماني الدولي

كيغالي، رواندا

11–15 تشرين الأول/أكتوبر 2022

اللجنة الدائمة
للسلم والأمن الدوليين

C-I/145/6-Inf.1
13 أيلول/سبتمبر 2022

جلسة استماع مع خبراء حول موضوع *الهجمات والجرائم الإلكترونية: المخاطر الجديدة على الأمن العالمي*

الجمعة، 14 تشرين الأول/أكتوبر 2022، 14:30 – 16:30
(قاعة MH1، الطابق الأرضي، مركز كيغالي للمؤتمرات (KCC))

مذكرة توضيحية

نعيش اليوم في حالة نزاعات عالمية واسعة النطاق. لا يمكن لأي حكومة أو برلمان في العالم أن يتوقع معاناة جميع مواطني كوكبنا في مواجهة جائحة مثل كوفيد-19.

واتخذت جميع الحكومات قراراً لحماية مواطنينا، بإخضاع ملايين الأشخاص في العالم لإجراءات تقييدية وفرض الإقفال التام.

ونتيجة للإقفال التام والبقاء في المنزل، ازداد الترابط بالشبكات، واقتناء الأجهزة، والكاميرات، وأجهزة الكمبيوتر، والهواتف الذكية للتمكن من الاتصال بالشركات والمدارس، أو ببساطة للتواصل مع العائلة والأصدقاء.

وسمحت الرقمنة القسرية للسكان بالحفاظ على روابط اجتماعية ومهنية تواصلية مع مراكز العمل، والمدارس والجامعات، وخاصة مع مؤسسات الصحة العامة، ووسائل الإعلام. ولذلك تمكن الناس في الوقت الحقيقي من معرفة تطور الجائحة، والتدابير التي يجري اتخاذها في بلدانهم.

ترجمة الأمانة العامة للاتحاد البرلماني العربي

وأتاحت الرقمنة السريعة، والقسرية مساحات جديدة لم يعرفها الكثير من الناس حتى الآن. ومع ذلك، ظهرت أيضاً مساحات جديدة أكثر خطورة على المستوى الفردي، والجماعي حيث قام مرتكبو الجرائم الإلكترونية بزيادة نطاق عملهم باستخدام أنظمة الهجمات الإلكترونية الجديدة.

ومن ناحية أخرى، أدى النزاع الخطير الذي نشهده في أوكرانيا إلى أعمال عدائية لم تشهدها أوروبا منذ الحرب العالمية الثانية. وكشفت أنه يمكن أيضاً استخدام الهجمات الإلكترونية لشن حرب في فترات التوتر الأقصى.

ويجب أن نعمل من أجل حظر الأسلحة الفتاكة المستقلة (المعروفة أيضاً باسم «الروبوتات القاتلة»)، وإعطاء الأولوية لحماية جميع البنية التحتية النووية من الهجمات الإلكترونية الخارجية المحتملة، ومنع تصعيد جديد في التهديد النووي العالمي.

وتستخدم حملات التضليل، والدعاية الضخمة المنصات الرقمية لتفسيد الجماعات، أو المناطق، أو البلدان والتأثير عليها. يتم تنفيذ الحملات من خلال نشطاء إلكترونيين منظمين يعرفون أنه يرد نقصاً في أطر التعاون القانوني الدولي.

وتعرّض للخطر الهجمات المباشرة على أنظمة الكمبيوتر ذات البنية التحتية المهمة في بلد ما شبكات التوزيع الأساسية للسلع الضرورية في مجتمعاتنا.

ويجب أن يجعلنا كل هذا نفكر ونتعمق أكثر في الواقع العالمي الذي يحيط بنا بصفتنا برلمانيين. أصبحت معرفة الحقيقة اليوم رصيداً ثميناً بشكل متزايد.

ويتطلب السياق الرقمي الجديد أيضاً عملاً من برلماناتنا ومن الأمم المتحدة. سيسمح ذلك بتعظيم فوائد وإمكانات مجتمع المعرفة لدينا، مع تقليل المخاطر الجسيمة التي تهددنا.

ووفقاً للمادة 19 من الإعلان العالمي لحقوق الإنسان، لكل فرد الحق في التماس الأنباء والأفكار وتلقّيها ونقلها إلى الآخرين، بأيّ وسيلة ودونما اعتبار للحدود. ولذلك، يجب أن نضمن أن يتمكن جميع المواطنين في مجتمعاتنا من الحصول بحرية على معلومات موضوعية وصادقة وجيدة النوعية.

وانطلاقاً من روح الإعلان العالمي لحقوق الإنسان، يجب أن نكفل تطور الخطاب العام بحيث، بدلاً من مواجهة، أو تقسيم، أو استقطاب، أو تدمير تعايشنا برسائل الكراهية الشائعة، يمكن أن تصبح ديمقراطياتنا أقوى.

ويجب أن يكون لدينا الحق في حماية بياناتنا ومعلوماتنا الشخصية، التي تُستخدم للتحكم بسلوكياتنا وتغييرها، والسيطرة علينا، وانتهاك حقوق الإنسان لدينا، وتقويض المؤسسات الديمقراطية.

وترد حاجة إلى تشريع لتحديد حدود الخوارزميات غير الشفافة، واستخدام الملفات الشخصية السيكوجرافية من قبل الشركات الكبيرة لمنع المنظمات الضارة، ومرتكبي الجرائم الإلكترونية من استخدام شبكات التواصل الاجتماعي للتأثير على اتجاهات الناخبين والتحكم بها.

ويجب أن نشجع القطاع العام، والقطاع الخاص، والمجتمع المدني على اعتماد أطر تشريعية، وتنظيمية ذاتية جديدة تطور حيزاً آمناً للتعاون الرقمي العالمي.

وبصفتنا برلمانيين، يجب أن ننشئ أطراً للتعاون القانوني الدولي لكي نتمكن من التصدي لمرتكبي الجرائم الإلكترونية الذين يعملون خارج أي نوع من السيطرة، والذين يمكنهم خدمة المصالح المظلمة لمهاجمة البنية التحتية المهمة في بلداننا.

وبما أن مرتكبي الجرائم الإلكترونية يدركون قيود قدرات البلدان على ملاحقتهم، فهم يعملون على النطاق العالمي، ويقومون بهجمات واسعة النطاق على المستخدمين. ينشرون جميع أنواع الهندسة الاجتماعية، وتقنيات الهجوم. وتشمل هذه: الاعتداءات على كلمات السر الشخصية، مثل الخداع الإلكتروني، والتصيّد الصوتي، والاحتيال عبر الرسائل النصية القصيرة ، والبريد الإلكتروني العشوائي (سبام)؛ والهجمات على الروابط، مثل شبكات الواي فاي الوهمية، والانتحال، وملفات تعريف الارتباط، وهجمات حجب الخدمة الموزعة، ولغة الاستعلام البنوية، والهجوم التشفيري؛ وهجمات البرامج الضارة، مثل الفيروسات، وبرامج الإعلانات المتسللة، وبرامج التجسس، وبرامج حصان طروادة، والأبواب الخلفية، وراصد لوحة مفاتيح (الكيلوغرز)، والاحتيال، وبرامج الفدية، والجذور الخفية، وشبكات الروبوتات (البوت نت)، وبرامج الأمان الخادعة، والاستغلال غير المشروع للحواسيب لتوليد النقود الرقمية، وغيرها من التطبيقات الضارة.

وفي العام 2015، اتخذ أعضاء الاتحاد البرلماني الدولي قراراً في الجمعية العامة في هانوي بشأن الحرب الالكترونية، التي تتصدى أيضاً للجرائم الالكترونية. ودعا القرار إلى إبرام اتفاقية دولية بشأن هذه الجرائم.

وأما بالنسبة لبرلماناتنا، فيجب أن نقدم هياكل تشغيلية قادرة على حماية القطاعات الضعيفة بشكل خاص (مثل النساء، والشباب، والأطفال، والشركات، والبنية التحتية المهمة) وأن نسعى إلى تطوير مبادرات تسمح لنا بتحديد الهجمات الإلكترونية، وكشفها، وتحليلها، ومنعها.

وفي سياق اتفاقية الجريمة الالكترونية، يمكن للاتحاد البرلماني الدولي، بل يجب عليه، أن يقدم مساهمة قيّمة للأمم المتحدة في الجهود العالمية الرامية إلى توفير الخدمات اللازمة لمنع حوادث الأمن الالكتروني في أي بلد من بلدان العالم، وزيادة الوعي بها وكشفها، والتصدي لها على النحو المناسب.

Inter-Parliamentary Union
For democracy. For everyone.

145th IPU Assembly

Kigali, Rwanda
11-15 October 2022

145th IPU ASSEMBLY
2022 | Kigali, Rwanda

Standing Committee on
Peace and International Security

C-I/145/6-Inf.1
13 September 2022

Expert hearing on the theme *Cyberattacks and cybercrimes: The new risks to global security*

Friday 14 October 2022, 14:30 – 16:30
(Room MH1, ground floor, Kigali Convention Centre (KCC))

Concept note

Today, we live in a situation of largescale global conflicts. No government or parliament in the world could foresee the suffering of all our planet's citizens in the face of a pandemic such as COVID-19.

To protect our citizens, all governments made the decision to subject millions of people in the world to restrictive measures and lockdowns.

As a result of being locked down at home, there was an increase in interconnections to networks and in the acquisition of devices, cameras, computers and smartphones to be able to connect to companies and schools, or simply to communicate with family and friends.

This enforced digitization allowed the population to maintain communicative social and professional links with work centres, schools and universities, and especially with public health institutions and the media. People were therefore able to learn in real time about the evolution of the pandemic and the measures being taken in their respective countries.

Rapid and enforced digitization has opened up new spaces that many people did not know about until now. However, at an individual and collective level, riskier new spaces have also appeared where cybercriminals have increased their scope of action using new cyberattack systems.

On the other hand, the serious conflict that we are witnessing in Ukraine has led to hostilities that Europe has not experienced since the Second World War. It has revealed that cyberattacks can also be used to wage war at periods of maximum tension.

We must work towards a ban on lethal autonomous weapons (also known as "killer robots"), prioritize the protection of all nuclear infrastructure from possible external cyberattacks, and prevent a new escalation in the global nuclear threat.

Massive disinformation and propaganda campaigns use digital platforms to contaminate and influence groups, regions or countries. The campaigns are delivered through organized cyber-activists who know that there is a lack of international legal cooperation frameworks.

Direct attacks on a country's critical-infrastructure computer systems put at risk the basic distribution networks for essential goods in our societies.

All this should make us reflect and delve deeper into the global reality that surrounds us as parliamentarians. Knowing the truth today is becoming an increasingly precious asset.

A new digital context also requires action from our parliaments and the United Nations. This will allow the benefits and potential of our knowledge society to be maximized, while minimizing the serious risks that threaten us.

According to article 19 of the Universal Declaration of Human Rights, everyone has the right to receive and impart information and ideas through any media, regardless of frontiers. Therefore, we must guarantee that all citizens in our societies can freely access objective, truthful and good-quality information.

In the spirit of the Universal Declaration of Human Rights, we must ensure public discourse develops so that, rather than confronting, dividing, polarizing or destroying our coexistence with viral hate messages, our democracies can grow stronger and stronger.

We must have the right to protect our data and personal information, which are used to manipulate and change our behaviours, control us, violate our human rights, and undermine democratic institutions.

Legislation is needed to define the limits of opaque algorithms and the use of psychographic profiles by large corporations so as to prevent malicious organizations and cybercriminals from using social networks to influence and manipulate the trends of voters.

We must encourage the public sector, the private sector and civil society to adopt new legislative and self-regulatory frameworks that develop a safe space for global digital cooperation.

As parliamentarians, we must establish international legal cooperation frameworks to be able to effectively combat cybercriminals who work outside any type of control and who can serve dark interests to attack critical infrastructure in our countries.

As they know the limitations of countries' abilities to pursue them, cybercriminals act globally, and develop largescale attacks on users. They deploy all kinds of social engineering and attack techniques. These include: attacks on personal passwords, such as phishing, vishing, smishing and spam; attacks on connections, such as fake wifi, spoofing, cookies, DDoS, SQL and sniffing; and malware attacks, such as viruses, adware, spyware, Trojans, backdoors, keyloggers, stealers, ransomware, rootkits, botnets, rogueware, cryptojacking and other malicious apps.

In 2015, IPU Members adopted a resolution at the Assembly in Hanoi on cyberwarfare, which also addressed cybercrime. The resolution called for an international convention on these crimes.

As for our parliaments, we must offer operational structures capable of protecting particularly vulnerable sectors (such as women, youth, children, companies and critical infrastructure) and seek to develop initiatives that allow us to identify, catalogue, analyse and prevent cyberattacks.

In the context of the Convention on Cybercrime, the IPU can and should make a valuable contribution to the United Nations in the global effort to provide services to prevent, raise awareness, detect and adequately respond to cybersecurity incidents in any country of the world.