



## ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD

Web: [www.issi.org.pk](http://www.issi.org.pk)  
Phone: +92-51-9204423, 24  
Fax: +92-51-9204658

### THE FIRST EVER UN SECURITY COUNCIL HIGH LEVEL OPEN DEBATE ON CYBER SECURITY: AN ASSESSMENT

By  
**Aamna Rafiq**  
Research Associate  
Arms Control & Disarmament Centre, ISSI

Edited by  
**Malik Qasim Mustafa**

September 28, 2021

*(Views expressed in the brief are those of the author, and do  
not represent those of ISSI)*



**“Digital technologies are increasingly straining existing legal, humanitarian and ethical norms, non-proliferation, international stability, and peace and security... These dynamics can encourage States to adopt offensive postures for the hostile use of these technologies. It can also enable non-state armed and criminal groups and individuals seeking to develop or access potentially destabilising capabilities with a high degree of impunity.”<sup>1</sup> This was said by Ms Izumi Nakamitsu, High Representative for Disarmament Affairs, at the United Nations Security Council (UNSC) Open Debate on Cyber Security: Maintaining international peace and security in cyberspace.**

The Prime Minister of the Republic of Estonia, Ms Kaja Kallas presided over the meeting. The US, UK, Russia, China, France, Ireland, Kenya, India, Mexico, Niger, Norway, Tunisia and Vietnam attended the meeting. The UNSC also invited all the member states of the UN that are not members of the Council and permanent observers to the UN to participate in the discussion through a written statement.<sup>2</sup> The objectives of this open debate were to: i) discuss the present and emerging cyber

<sup>1</sup> United Nations, Office for Disarmament Affairs, *UN Security Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace*, Remarks by Ms. Izumi Nakamitsu High Representative for Disarmament Affairs, June 29, 2021, <https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Nakamitsu-29-June.pdf>

<sup>2</sup> United Nations, Permanent Mission of Estonia to the UN, *UN Security Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace*, Concept Note, accessed on July 10, 2021, <https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Concept-note-UNSC-open-debate-on-cybersecurity-29.06.2021.pdf>

threats to international security; ii) analyse the general as well as the humanitarian impact of potential misuse of cyber technologies during the future-armed conflicts; iii) recognise the existing mechanisms at national, regional and global levels for the promotion of responsible state behaviour and mitigation of threats in cyberspace; iv) identify the ways to improve the state compliance with the existing international law and implementation of the UN norms of responsible state behaviour in cyberspace; v) examine the role of all key stakeholders for cyber resilience, confidence-building measures and conflict prevention.<sup>3</sup>

The *UN Security Council High Level Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace* is a major development of great significance because it is the first time the Council has discussed cybersecurity in a formal open debate setting. Although the UNSC has broadly discussed the malicious use of cyberspace in its various informal discussions and Aria-Formula meetings, it has never taken up cybersecurity as a stand-alone issue until now. As one of the six main organs of the UN established under a mandate of the UN Charter, the UNSC is primarily responsible for maintaining international peace and security, developing friendly relations among nations, promoting respect for human rights and resolving existing conflict and crisis.<sup>4</sup> During the 76 years of its establishment, the UNSC has mostly dealt with the traditional issues that affect international peace and security. It has previously deliberated on some new and emerging challenges to international peace and stability like climate change, pandemic, piracy, etc. However, introducing a new issue at UNSC, let alone the formal discussion, is extremely difficult.

Despite a broader consensus among participating states on the growing impact of digitalisation on human civilisation and the threats posed by increasing malicious cyber activities to every facet of it, a long-standing and controversial difference on the issues of applicability of existing international law and cyber sovereignty were quite visible in the meeting. These were among the major issues that previously caused a five-year deadlock from 2015 to 2020 at the Group of Governmental Experts platform. In their official statements, the states of the Western block e.g. the US, EU, Nordic countries and India reaffirmed their support for the applicability of existing international law in its entirety. This includes international human rights, international humanitarian law and the UN Charter. They also pledged to protect the freedom of the internet along with the freedom of assembly, association and expression in cyberspace.<sup>5</sup> The critical aspects of this stance faced

---

<sup>3</sup> Ibid.

<sup>4</sup> United Nations, "What is the Security Council?" accessed on July 12, 2021, <https://www.un.org/securitycouncil/content/what-security-council>

<sup>5</sup> Delegation of the European Union to the United Nations, *EU Statement – United Nations Security Council: Open Debate on Cyber Security*, New York, June 29, 2021, [https://eeas.europa.eu/delegations/un-new-york/100957/eu-statement-%E2%80%93-united-nations-security-council-open-debate-cyber-security\\_en](https://eeas.europa.eu/delegations/un-new-york/100957/eu-statement-%E2%80%93-united-nations-security-council-open-debate-cyber-security_en);

opposition from the states of the other block especially Russia and China. In its official statement,<sup>6</sup> Russia supported the concept of cyber sovereignty by stating that every state must have the right to regulate its own digital space and infrastructure in accordance with its own security needs. It further stated that it does not consider cyberspace as an entirely unregulated space but the debate on how the existing law will be applied in the cyber domain is “far from close” as there is no such thing as “automatic application.” Without naming any specific state, Russia said that few technologically advanced states are attempting to twist the debate in the direction of imposing their “rules of the game” on all other members. Russia expressed its concerns regarding manipulation of international law for imposing unilateral pressures, sanctions and conducting “preventive military cyber strikes.”<sup>7</sup> The principality of Liechtenstein also highlighted the concern of similar nature regarding the applicability of Article 51 of the UN Charter.<sup>8</sup> In its official statement, China also emphasised respecting the right of all states to independently design their internet governance model.<sup>9</sup>

Pakistan attended the open debate as an observer state. Pakistan attaches great importance to the issue of cybersecurity and the UN’s role as a key platform. Pakistan views the progress in the field of cyber technologies as a driver of social and economic prosperity and growth. However, it is also cognisant of the challenges and threats posed by the misuse of dual-use cyber technologies by the state and non-state actors for their malicious objectives, putting international peace and security at risk. Pakistan holds a view that the existing international law and the UN Charter provide a “fundamental and guiding framework” for the states regarding the use of these technologies. However, keeping in view the unique virtual nature of cyberspace and the level of speed, stealth and anonymity that comes with it, there is a need to reconsider certain aspects of existing international law. Therefore, states must refrain from interpreting the applicability of existing international law in the cyber domain as it could aggravate the cyber conflicts. Pakistan considers the concerns of states regarding the applicability of Article 51 of the UN Charter to the cyber domain as legitimate which must be addressed. Pakistan also believes that principles of sovereignty, sovereign quality, peaceful

---

United States Mission to the United Nations, *Remarks by Ambassador Linda Thomas-Greenfield at a UN Security Council Open Debate on Cybersecurity*, June 29, 2021, <https://usun.usmission.gov/remarks-by-ambassador-linda-thomas-greenfield-at-a-un-security-council-open-debate-on-cybersecurity/>

<sup>6</sup> Permanent Mission of the Russian Federation to the United Nations, *Statement by Permanent Representative Vassily Nebenzia at an open VTC of UNSC Members on Maintenance of International Peace and Security: Cyber Security*, June 29, 2021, <https://russiaun.ru/en/news/inf29062021>.

<sup>7</sup> Ibid.

<sup>8</sup> Permanent Mission of the Principality of Liechtenstein to the United Nations, *Security Council - High-Level Open Debate on Maintaining International Peace and Security in Cyberspace*, June 29, 2021, <https://twitter.com/LiechtensteinUN/status/1409897230144843782>.

<sup>9</sup> Chinese Mission to the United Nations, *Remarks by Amb. Zhang Jun at Security Council Open Debate on Cyber Security*, June 29, 2021, [https://www.fmprc.gov.cn/mfa\\_eng/wjb\\_663304/zwjg\\_665342/zwbd\\_665378/t1888053.shtml](https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbd_665378/t1888053.shtml).

settlement of disputes and non-interference in the internal affairs of the states must be observed in all domains, including cyberspace.<sup>10</sup>

All states accepted the importance of cyberspace for social, political and economic development. They expressed their desire for peace, stability, security and expressed their concerns regarding increasing protectionism, extremism, militarisation, politicisation, disinformation and terrorism in cyberspace. In order to enhance compliance, promote responsible state behaviour and conflict prevention in cyberspace, states came up with various constructive recommendations. The US is more inclined towards using the rules and framework provided in the previous reports of the UNGGE process while Russia is looking forward to the working of the OEWG for the next four years. The EU supported the formulation of confidence-building measures at the regional and international level to minimise the risk of crisis escalation and misinterpretation in case of any cyber conflict in future. Furthermore, the EU stressed increasing the scale and scope of efforts in the field of cyber diplomacy for capacity building, improving global multi-stakeholder cooperation and reducing the gender digital divide. In addition to other western states, the EU encouraged other states to support the proposal of the Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA). PoA, if established, will provide a permanent and institutionalised UN mechanism for designing a comprehensive cyberspace regime. Pakistan stresses the development of binding rules for responsible state behaviour in cyberspace to minimise the threat of weaponisation and promote the peaceful uses of ICTs. Pakistan also supports the idea of establishing an international, inclusive and institutionalised platform within the UN system for negotiating agreements, capacity-building mechanisms, CBMs, regular institutional dialogue and transparent exchange of information and best practices.<sup>11</sup> Although every recommendation has its pros and cons, all these recommendations are steps in the right direction. States can either start working on all recommendations at once or adopt a one-step at a time approach but agreeing to bridge the gaps, reach consensus and achieve unity in good faith for global good is a pressing necessity above all.

---

<sup>10</sup> Pakistan Mission to United Nations, *Working Paper by Pakistan for Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, March 12, 2021.

<sup>11</sup> Ibid.