



Mr. Karim A.A. Khan KC
Prosecutor
International Criminal Court
The Hague
The Netherlands

Oslo, 11 October 2023

Esteemed Mr. Prosecutor,

The Norwegian Helsinki Committee would like to raise concerns related to media reports about a serious cyber security incident at the ICC.

In a statement on X (formerly Twitter) of 19 September 2023, the ICC stated that “at the end of last week, the International Criminal Court’s services detected anomalous activity affecting its information systems. Immediate measures were adopted to respond to this cyber security incident and to mitigate its impact.”¹ The statement underlines that the Court is in the process of “strengthen[ing] its cybersecurity framework, including accelerating its use of cloud technology.”

Media reports include articles in the Business Standard,² NL Times,³ Arabiya News,⁴ and Reuters,⁵ describing the situation as serious, disrupting employees’ access to e-mail, documents, and the internet. Reports suggest but do not confirm that sensitive information related to any of the Court’s situations has been compromised.

We work closely with local organizations in Ukraine and other situations where core international crimes have been committed. Since the establishment of the ICC, we have advised our local partners to cooperate with the Court and share relevant information with your Office, a practice that we have followed ourselves. We have done so on the assumption that the ICC has safe storage systems and that by sending sensitive information we would

¹ <https://twitter.com/IntlCrimCourt/status/1704118503630872887>

² “ICC war crimes tribunal hobbled by hacking incident”, 21 September 2023, The Business Standard (<https://bit.ly/3RKYqDx>).

³ “Cyber-attack on International Criminal Court in The Hague; Hackers stole sensitive docs”, NL Times, 20 September 2023 (<https://bit.ly/3PDyKzX>).

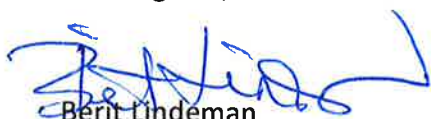
⁴ “International Criminal Court hobbled by hacking incident”, Alarabiya News, 21 September 2023 (<https://bit.ly/48HzfYW>)

⁵ “War crimes tribunal ICC says it has been hacked”, Reuters, September 19, 2023 (<https://bit.ly/46ejAON>).

not in any way jeopardize the safety of victims, witnesses or civil society organizations involved in fact-finding work.

Considering the recent cyber-attack against the Court, we would like to ask whether the Court has by now diagnosed the attack, the scope of compromised information, and the technical nature of the intrusion. While we appreciate that the attack may be under criminal investigation, transparency about the diagnosis is essential, especially vis-à-vis victims and NGOs that have submitted information to your Office. Until we have heard from you on this matter, we are compelled to pause the submission of potential evidence to your Office and to ask our partners in situation countries to do the same.

Best regards,



Berit Lindeman
Secretary General



Gunnar M. Ekeløve-Slydal
Deputy Secretary General