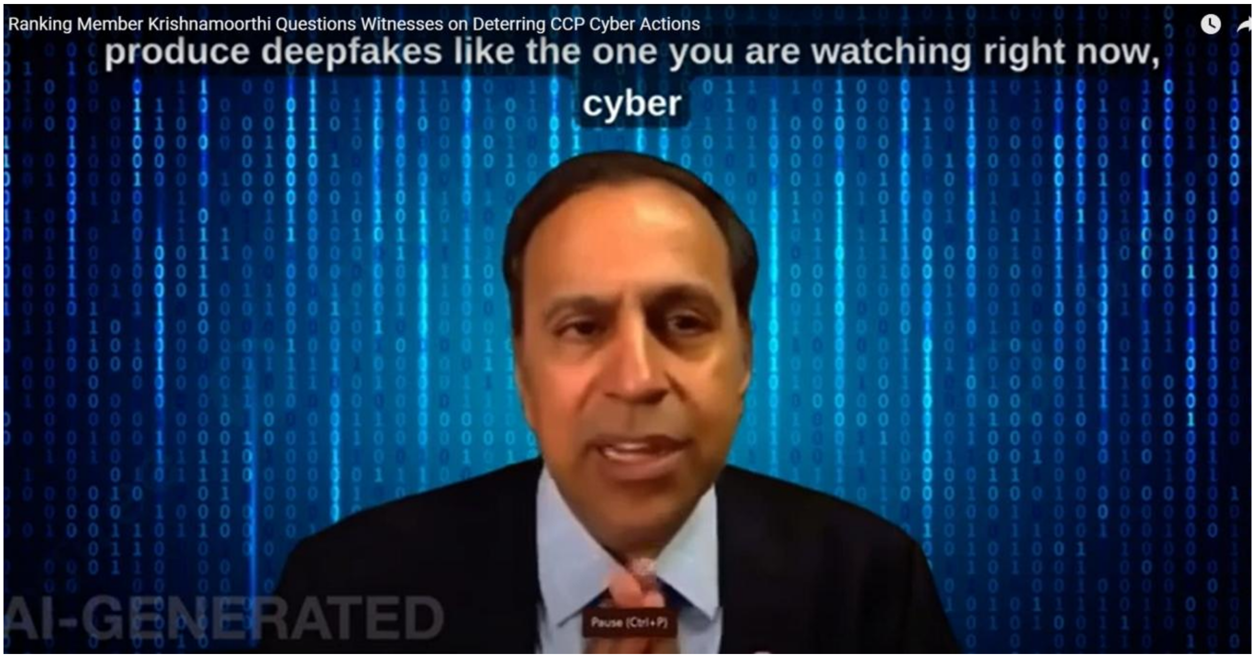
SELECT COMMITTEE ON THE CCP
DEMOCRATS | RANKING MEMBER RAJA KRISHNAMOORTHI

July 14, 2025

The Honorable Marco Rubio
United States Secretary of State
Department of State
2201 C Street Northwest
Washington, DC 20520

Dear Secretary Rubio:

Earlier this year, I posed what, to the best of my knowledge, was the first-ever congressional hearing question asked via deepfake. This occurred at the Select Committee's March 2025 hearing on cyber threats involving the Chinese Communist Party (CCP). A screenshot of "Deepfake Raja" from my question line is pictured below.



Ranking Member Krishnamoorthi Questions Witnesses on Deterring CCP Cyber Actions

produce deepfakes like the one you are watching right now,
cyber

One of the points I was trying to make through this demonstration was that bad actors could use deepfakes to impersonate senior political leaders and spread disinformation, which could cause great harm to our foreign policy. According to recent news reports, it appears a version of my concern may have just materialized. Per these reports, "[t]he State Department is warning U.S. diplomats of attempts to impersonate Secretary of State Marco Rubio and possibly other officials using technology driven by artificial intelligence . . . The warning came after the Department discovered that an impostor posing as Rubio had attempted to reach out to at least three foreign ministers, a U.S. senator and a governor."[1] Others have noted that this may be "one of the most audacious examples yet of AI-enabled political deception . . .[given that it involved] AI deepfake tools to impersonate [Secretary Rubio's] voice and writing style in a series of targeted communications."[2] Separate reporting indicates that the State Department is "aware of this incident and is currently investigating the matter."[3]

While I currently have no information indicating this incident involved a foreign state, and hoaxers are equally capable of creating deceptive deepfakes like this given the proliferation of AI technologies, this incident presents an opportunity to highlight such risks and seek information about the Department's efforts to counter them.

This is not a new concern. In fact, in 2019, the first-ever federal statute on deepfakes was enacted.[4] It required, among other things, the U.S. Government to assess how "foreign governments, including foreign intelligence services, foreign government-affiliated entities, and foreign individuals, could use or are using machine-manipulated media . . . to harm the national security interests of the United States, including [any] historic, current, or potential future efforts of China and Russia to use machine-manipulated media."[5]

As the Ranking Member of the House Select Committee on the Strategic Competition between the U.S. and the CCP, I share these concerns, especially as they relate to these countries of concern. It is particularly important to understand how deepfakes could be utilized to harm our national security, including by creating fake diplomatic incidents and even distorting decision-making during times of conflict. Given the CCP's efforts to dominate artificial intelligence, these are not possibilities that should be dismissed lightly in the context of countries like China.

Accordingly, I request answers to the following questions by no later than August 1, 2025.

1. Please provide a detailed description of the recent incident involving Secretary Rubio, including a description of the content of the AI-generated impersonated communications and any information regarding the hoaxer or other threat actor suspected to be behind this incident.
2. Please describe any ongoing efforts of the State Department to prevent the future impersonation of senior officials using AI, including any efforts to adopt content authentication protocols or otherwise build greater trust in official State Department communications.

[1] Matthew Lee, "Imposter uses AI to impersonate Rubio and contact foreign and US officials," *The Washington Post,* 7/8/2025. https://www.washingtonpost.com/politics/2025/07/08/rubio-artificial-intelligence-impersonation/.

[2] Anthony Kimery, "AI voice deepfake of U.S. Secretary of State triggers global security alert," *Biometric Update*, 7/8/2025 https://www.biometricupdate.com/202507/ai-voice-deepfake-of-u-s-secretary-of-state-triggers-global-security-alert.

[3] Edward Wong, "Marco Rubio Impersonation Under State Dept. Investigation," *The New York Times*, 7/8/2025. https://www.nytimes.com/2025/07/08/us/politics/rubio-ai-impersonation-investigation.html.

[4] David Dorfman, "Decoding Deepfakes: How Do Lawyers Adapt When Seeing Isn't Always Believing?" *Oregon State Bar Bulletin*, pg. 18-24, 4/2020. https://www.osbar.org/bulletin/issues/2020/2020April/offline/download.pdf.

[5] 50 U.S.C. §§3369a.

3. Has the State Department engaged in any planning or other analysis to help mitigate the risk that deepfakes could trigger diplomatic incidents or result in faulty intelligence judgments, particularly in the context of U.S.-PRC relations?
4. Does the State Department have an official process or procedure to adjudicate the authenticity of videos or other messages purporting to be from foreign senior officials, including senior officials of the PRC?
5. Is the State Department monitoring the efforts of the CCP and PRC-based companies to develop the most advanced generative AI tools, including deepfake-generation technologies?
6. Does the State Department agree that PRC-based generative AI companies and the technologies they produce present a profound national security risk in the hands of the PRC or other similarly-situated nations, and if so, what if any actions are under consideration to address such concerns?

Thank you for your attention to this matter.

Sincerely,

Raja Krishnamoorthi

Raja Krishnamoorthi
Ranking Member