ELIOT L. ENGEL, NEW YORK
CHAIRMAN

JASON STEINBAUM
STAFF DIRECTOR

MICHAEL T. MCCAUL, TEXAS
RANKING REPUBLICAN MEMBER

BRENDAN P. SHIELDS
REPUBLICAN STAFF DIRECTOR

One Hundred Sixteenth Congress

U.S. House of Representatives

Committee on Foreign Affairs

2170 Rayburn House Office Building
Washington, DC 20515
www.foreignaffairs.house.gov

July 8, 2020

The Honorable Michael R. Pompeo
Secretary
United States Department of State
2201 C Street NW
Washington, DC 20520

Dear Mr. Secretary:

I write to raise serious concerns about the growing rate of cybercrime impacting the American people and our public and private sector institutions during the COVID-19 crisis and to request information regarding the Department's efforts to respond to the international aspect of these threats and boost international cooperation to bring the perpetrators to justice.

The United States is seeing an unprecedented cybercrime wave as more Americans than ever are reliant on technology for their everyday activities as the COVID-19 virus continues to spread. The FBI has reported a quadrupling of daily reports of cybercrime as criminals, many of whom are not located in the United States, look to exploit the pandemic and the vulnerabilities related to remote work. Nation-states, too, are turning to cybercrime to seek out information about America's response to COVID-19. In particular, I am deeply concerned about increasing reports of criminals stealing stimulus payments at a time when the pandemic has already caused tremendous personal and economic hardship for all Americans.[1] The Secret Service recently testified before Congress that it expects more than $30 billion in COVID-19 stimulus funds to be lost to cybercrime alone,[2] and the Offices of Inspector General across the government recently reported that cybercrime and other cybersecurity threats are a top challenge in the COVID-19 response.[3] The targeting of critical infrastructure, especially hospitals and vaccine development labs, in the United States and around the globe during the pandemic is appalling and demonstrates that criminals and nation-states perpetrating these cyberattacks are motivated not just by profit but also the acquisition of intelligence about virus responses.

---

[1] https://www.nytimes.com/2020/04/22/technology/stimulus-checks-hackers-coronavirus.html
[2] https://www.judiciary.senate.gov/imo/media/doc/D'Ambrosio%20Testimony.pdf
[3] https://www.oversight.gov/sites/default/files/oig-reports/Top%20Challenges%20Facing%20Federal%20Agencies%20-%20COVID-19%20Emergency%20Relief%20and%20Response%20Efforts.pdf

These malicious cyber activities are unacceptable and the criminals behind them must face consequences for their actions. Unfortunately, some estimates indicate as few as 3 in 1,000 cybercrime incidents that occur in the United States ever see an arrest of the perpetrator.[4] This enforcement gap may be exacerbated by what the United Nations Office on Drugs and Crime recently assessed will be a reduction in the number of global law enforcement personnel focused on cybercrime and digital evidence as many are diverted to other COVID-19 priorities or become ill with the virus themselves.[5]

Against this backdrop, the Department of State plays a critical role in working with our federal law enforcement authorities to facilitate international cooperation on cybercrime, strengthen the capacity of governments to work with us in bringing cybercriminals to justice, and establish and enforce norms of responsible state behavior in cyberspace. Congress has largely supported these efforts and has provided $10 million in funding annually through the State and Foreign Operations Appropriations Bill for global cybercrime and IPR programming to help boost the capabilities of other governments to, among other things, support the United States in investigating and prosecuting cybercrime. I am disappointed that the FY 2021 budget request proposed to cut this modest amount of funding in half at a time where cybercrime is hitting more Americans than ever before. Additionally, while I appreciated your statement that the US government will work to promote nonbinding norms regarding states refraining from malicious cyber activity that intentionally damages critical infrastructure, I would welcome further information about US efforts to encourage governments to adhere to nonbinding norms concerning how best to assist countries like the United States in prosecuting cybercrime.

In light of the COVID-19 pandemic and the increasing cybercrime wave seen during this crisis, I ask you to provide the Committee with the following information:

1. What steps is the Department of State taking to strengthen and expand its support to other governments and international organizations to improve their capacity to go after the cybercriminals that are targeting Americans during this crisis and how has this work been impacted by restrictions on in-person interactions?

2. What steps is the Department of State taking to increase cooperation between State Department personnel and the FBI and other US law enforcement authorities to boost US efforts to bring foreign cybercriminals to justice and rapidly respond to requests for assistance from other governments to address cybercrime?

3. What further steps will the Department of State take, including in ongoing norms processes, to encourage and compel other governments to cooperate with the United States in efforts to impose consequences on cybercriminals operating in their territory?

---

[4] https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors

[5] https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf

4. How is this rise on cybercrime during the COVID-19 pandemic impacting the Department of State's strategy regarding the possible negotiations of a global cybercrime treaty advocated for by Russia?

As the COVID-19 virus continues to ravage the United States, I hope you will agree that identifying, stopping, and bringing to justice the cybercriminals exploiting the pandemic to attack our people, governments, businesses, and other critical institutions must be a core priority for the Department of State. This will not be possible without the cooperation of our foreign partners, many of which benefit from our country's legal and technical assistance. I look forward to hearing how the Department is strengthening and expanding its efforts to boost this cooperation and combat the global cybercrime wave.

Sincerely,

Eliot L. Engel

ELIOT L. ENGEL
Chairman