Congress of the United States
Washington, DC 20515

April 5, 2022

The Honorable President Joseph R. Biden
President of the United States
The White House
Washington DC 20500

Dear Mr. President,

We write regarding your Administration's efforts to cooperate with our international partners and allies to secure cyber defenses against cyberattacks by Russia and other malign actors. We appreciate the precautions taken thus far, principally through the Cybersecurity and Infrastructure Security Agency (CISA), to actively prepare U.S. businesses and critical infrastructure for possible Russian cyberattacks, including your Administration's recent warnings that Russia may attempt to conduct cyberattacks in retaliation for the economic penalties the United States and our allies and partners imposed in response to the Russian war against Ukraine.[1] To complement those efforts, we urge your Administration to increase assistance to our Ukrainian and European allies for the purpose of hardening defenses against cyberattacks, and to promptly nominate an Ambassador-at-large to lead the State Department Bureau of Cyberspace and Digital Policy, which the Department officially stood up this week.

We have watched in horror as Russia wages an unprovoked war against Ukraine, targeting civilians and cities indiscriminately through ground artillery and aerial bombardment. Thus far, Russia has primarily employed conventional weapons in the conflict; where it has used cyber-weapons, they have proven largely ineffective. Earlier in the war, for example, the United States attributed to the Russian and Belarusian governments denial of service attacks on Ukrainian banks and government websites, "wiper" attacks intended to destroy critical files, and malware attacks intended to disrupt Ukrainian government websites.[2] Fortunately, U.S. Cyber Command, the U.S. Commerce Department, our European allies, and private industry appear to have worked to help Ukraine deny Russia any significant advantage through these cyberattacks.[3] But as Russian forces remain stalled, President Vladimir Putin may be adopting more desperate tactics. On March 29, for example, Ukraine's state-run telecommunications provider suffered a massive cyberattack that reduced user connectivity levels to 13% of pre-war levels and took multiple hours to mitigate.[4] Ukraine said Russia was responsible for the attack. The robust response in Ukraine, so far, is a test case for the scope of collaboration we need to replicate with other U.S. allies and partners to detect, attribute, and respond to cyberattacks.

---

[1] Maegan Vazquez et al., *Biden warns business leaders to prepare for Russian cyber attacks,* CNN (Mar. 21, 2022), https://www.cnn.com/2022/03/21/politics/biden-russia-cyber-activity/index.html.
[2] Mehul Srivastava et al., *The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion,* Financial Times (Mar. 9, 2022), https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471.
[3] *Id*.
[4] Ada Petriczko, *A major Ukrainian internet provider reports a cyberattack*, N.Y. Times (Mar. 29, 2022), https://www.nytimes.com/live/2022/03/28/world/ukraine-russia-war#major-ukrainian-internet-provider-reports-a-cyberattack.

Ukraine's inspiring resistance in thwarting Russia from achieving its strategic objectives may lead President Putin to unleash cyberattacks on a larger scale — one that exacerbates the humanitarian crisis in Ukraine or tests the boundaries of what the NATO alliance considers an armed attack under Article V of its Charter. To that end, we strongly urge you to immediately nominate an Ambassador-at-large to head the State Department's newly created Bureau of Cyberspace and Digital Policy, and provide the Bureau with appropriate staffing and resources. By establishing a single cyber diplomatic point of contact to help allies and partners bolster their own defenses, this Bureau will fill a crucial gap in our cyber support structures spread across U.S. government agencies. The Cyber Bureau can work towards strengthening the eleven voluntary norms included in the 2015 report of the UN Government of Experts, which the UN General Assembly later adopted.[5] Specifically, we urge you to ensure that the Bureau will promote the values of an interoperable, open, and secure internet, and work to increase the diplomatic and economic costs of defying international norms of acceptable behavior in the cyber domain.

We are clear-eyed about the effectiveness of voluntary international norms. By themselves, such norms may not deter actors in Russia, China, Iran, and North Korea from launching cyberattacks against the United States, our allies, and our partners. Punishment through sanctions likewise may not change the calculus of a determined adversary such as Russia. However, by clearly establishing the severe consequences for cyberattacks against critical infrastructure — including the food supply, nuclear command and control, and the electrical grid — we raise the expected costs of undertaking such an attack. For instance, we encourage your Administration to bolster deterrence by outlining the range of possible policy options in response to cyberattacks, much as the European Union has done through its "Cyber Diplomacy Toolbox."[6]

The threat of significant cyberattacks grows greater by the day. We, therefore, request that by April 29, 2022, you respond in writing to the following questions concerning our defenses against Russian cyberattacks and your Administration's overall approach to cyber diplomacy.

1. What lessons have we learned from the Russian government cyberattacks against Ukraine to date? How is the Administration coordinating U.S. government agencies to apply these lessons to shore up potential U.S. vulnerabilities as well as those of our allies and partners?

2. What criteria would the Administration use to determine whether a cyberattack on a NATO member should trigger Article V of the North Atlantic Charter on collective self-defense?

3. Approximately what is the timeline to fully staff up the new Bureau? How will the Bureau of Cyberspace and Digital Policy work with other U.S. government agencies and

[5] Chris Jailkaran, *Cybersecurity: Deterrence Policy,* CRS Report (Jan. 18, 2022), https://crsreports.congress.gov/product/pdf/R/R47011.
[6] Erica Moret & Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?,* EUISS Brief (July 2017), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf.

international partners to build capacity to help deny, deter, and impose costs on malign actors who conduct cyberattacks?

4. Which federal agencies currently engage with other countries to defend against cyberattacks? How are these agencies coordinating a whole-of-government approach to deter and, if necessary, respond to Russian cyberattacks? For instance, how will the State Department's Bureau of Cyberspace and Digital Policy work with agencies that already have a global engagement function, particularly CISA, which published a "CISA Global" Strategy in 2021?

5. Will the Administration outline the scope of possible policy responses to cyberattacks on the United States as the European Union has done?

6. Under what circumstances would the Administration support the negotiation of a legally binding international treaty to complement non-binding norms to promote the peaceful uses of cyberspace?

7. How will the State Department evaluate progress towards the further development of the eleven norms of behavior set out in the 2015 report of the Group of Government Experts?

We commend your Administration for taking several steps to shore up cyber vulnerabilities that threaten the security of Ukraine and our allies. Your administration has worked in quiet ways to harden Ukraine's cyber defenses, and those of our European allies and partners, against a highly sophisticated cyber adversary in Russia. Nonetheless, cyberspace remains largely devoid of rules of the road, which adversaries such as Russia will continue to eagerly exploit. While our eyes remain on defending Ukraine in all domains of warfare, we also need U.S. leadership through an empowered State Department to reduce the risk that we find ourselves in a "real shooting war" due to a "cyber breach of great consequence,"[7] as you have cautioned.

Thank you in advance for your attention to this important matter.

Sincerely,

Edward J. Markey
United States Senator
Chairman, Senate Foreign Relations
Subcommittee on East Asia, Pacific,
and International Cybersecurity Policy

William R. Keating
Member of Congress
Chairman, House Foreign Affairs
Subcommittee on Europe, Energy,
the Environment and Cyber

[7] Shannon Vavra, *Biden Warns a 'Real Shooting War' Could Come From Cyber Breach,* The Daily Beast (Jul. 28, 2021), https://www.thedailybeast.com/biden-warns-a-real-shooting-war-could-come-from-cyber-breach.