



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

AUG 06 2021

The Honorable Kamala D. Harris
President
United States Senate
Washington, DC 20510

Dear Madam President:

On behalf of the Administration, I am pleased to present a legislative proposal for Congress' consideration—the Cybercrime Mitigation Act—that would (1) authorize courts to issue injunctions to stop damage to 100 or more computers; (2) clarify that the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, prohibits the sale or renting of a botnet; and (3) update Section 1030’s criminal and civil forfeiture provisions, which would help the federal government seize infrastructure used by cybercriminals. In its March 2020 final report, the Cyberspace Solarium Commission—a bipartisan commission of legislators, senior executive agency leaders, and nationally recognized experts from outside of government—called for Congress to enact legislation to provide courts with broader authority to disrupt all types of malicious botnets. This bill would be a significant step toward that goal.

Large-scale cybercrime, which involves damage to 100 or more computers in one year, is a significant threat to public safety and national security. For example, cybercriminals have used botnets (networks of compromised computers under a malicious actor’s control) to impersonate others and spread spam and phishing emails, and nation-state actors have used botnets to carry out malicious cyber activities. Criminals have also used servers to conduct distributed denial of service (DDoS) attacks to take down company websites and networks.

While the federal government has been able to successfully dismantle some large-scale cybercrime operations in the past, via injunctions, the authority of federal courts to enjoin these activities is limited to wiretap and fraud offenses. But cybercriminals damage computers during other types of illegal activity as well. For example, cybercriminals may steal sensitive corporate information or execute distributed denial of service (DDoS) attacks. Depending on the facts of a given case, these crimes may not constitute fraud or illegal wiretapping and thus could not be enjoined.

The Cybercrime Mitigation Act would fill this gap by granting courts the authority to enjoin a greater range of botnets and other cybercrime involving damage to 100 or more computers. This authority could be used to stop ongoing ransomware attacks—for example, to

dismantle a botnet that spreads ransomware along with other destructive malware—or to take down servers that are conducting DDoS attacks.

Another provision of this bill would explicitly criminalize the sale and renting of botnets. Botnets can provide criminal actors and adversaries with the means to amplify their malicious activities. Prohibiting the sale and renting of botnets would give the Department another tool to combat cybercriminals who provide “Infrastructure-as-a-Service” for malicious purposes.

Additionally, the legislation would update the CFAA’s criminal and civil forfeiture provisions. The new provisions would enhance the Department’s ability to dismantle, disrupt, and deter malicious cyber activity, and to target the instruments of, and profits from, cybercrime.

Thank you for the opportunity to present this proposal. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration’s program, there is no objection to submission of this letter.

Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Joe Gaeta
Deputy Assistant Attorney General



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

AUG 06 2021

The Honorable Nancy Pelosi
Speaker of the House
U.S. House of Representatives
Washington, DC 20515

Dear Madam Speaker:

On behalf of the Administration, I am pleased to present a legislative proposal for Congress' consideration—the Cybercrime Mitigation Act—that would (1) authorize courts to issue injunctions to stop damage to 100 or more computers; (2) clarify that the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, prohibits the sale or renting of a botnet; and (3) update Section 1030’s criminal and civil forfeiture provisions, which would help the federal government seize infrastructure used by cybercriminals. In its March 2020 final report, the Cyberspace Solarium Commission—a bipartisan commission of legislators, senior executive agency leaders, and nationally recognized experts from outside of government—called for Congress to enact legislation to provide courts with broader authority to disrupt all types of malicious botnets. This bill would be a significant step toward that goal.

Large-scale cybercrime, which involves damage to 100 or more computers in one year, is a significant threat to public safety and national security. For example, cybercriminals have used botnets (networks of compromised computers under a malicious actor’s control) to impersonate others and spread spam and phishing emails, and nation-state actors have used botnets to carry out malicious cyber activities. Criminals have also used servers to conduct distributed denial of service (DDoS) attacks to take down company websites and networks.

While the federal government has been able to successfully dismantle some large-scale cybercrime operations in the past, via injunctions, the authority of federal courts to enjoin these activities is limited to wiretap and fraud offenses. But cybercriminals damage computers during other types of illegal activity as well. For example, cybercriminals may steal sensitive corporate information or execute distributed denial of service (DDoS) attacks. Depending on the facts of a given case, these crimes may not constitute fraud or illegal wiretapping and thus could not be enjoined.

The Cybercrime Mitigation Act would fill this gap by granting courts the authority to enjoin a greater range of botnets and other cybercrime involving damage to 100 or more computers. This authority could be used to stop ongoing ransomware attacks—for example, to

dismantle a botnet that spreads ransomware along with other destructive malware—or to take down servers that are conducting DDoS attacks.

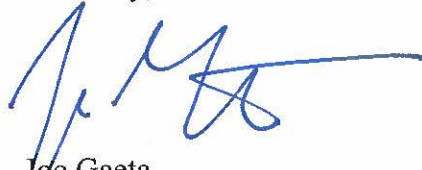
Another provision of this bill would explicitly criminalize the sale and renting of botnets. Botnets can provide criminal actors and adversaries with the means to amplify their malicious activities. Prohibiting the sale and renting of botnets would give the Department another tool to combat cybercriminals who provide “Infrastructure-as-a-Service” for malicious purposes.

Additionally, the legislation would update the CFAA’s criminal and civil forfeiture provisions. The new provisions would enhance the Department’s ability to dismantle, disrupt, and deter malicious cyber activity, and to target the instruments of, and profits from, cybercrime.

Thank you for the opportunity to present this proposal. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration’s program, there is no objection to submission of this letter.

Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,



Joe Gaeta
Deputy Assistant Attorney General