

**Congress of the United States**  
**Washington, DC 20515**

April 6, 2017

Secretary Steven T. Mnuchin  
U.S. Department of the Treasury  
1500 Pennsylvania Avenue, NW  
Washington, DC 20220

Dear Secretary Mnuchin,

We write to you today to express our concerns about the rapid spread of cyber-attacks on the American banking and financial service industries by foreign actors. It was reported earlier this week that Lazarus, a hacking operation connected to the North Korean regime, targeted banks in 18 different countries to illicitly fund the development of North Korea's long-range nuclear missile system. Among those harmed by these attacks was the Bangladeshi Central Bank which had \$81 million stolen from their account at the Federal Reserve Bank of New York last year.

These high profile attacks are symptomatic of a shift in North Korean hacking strategy from destroying systems to directly acquiring funds. Today, roughly 2,000 hackers in the employ of the North Korean regime live and work abroad to conduct cyber-attacks against banks and financial services groups, other businesses and defectors. South Korean cybersecurity experts have detected an increase in ransomware attacks on defectors and businesses in South Korea. This is deeply troubling. Cyber-attacks have become lucrative business. According to the FBI, cyber-criminals made over \$1 billion in 2016 through ransomware attacks alone. The gains from such attacks fund the development of increasingly sophisticated malware and other next generation cyber-attack tools. For rogue states like North Korea, we are concerned that these attacks will help fund missile tests and the development of nuclear weapons.

As Congress continues to investigate our nation's exposure to state sanctioned cyber-attacks on critical national infrastructure including our election systems and banks, it is imperative that the Treasury Department do all it can to keep our banking sector safe from these threats.

As the Ranking Members of the Oversight and Government Reform Subcommittee on Information Technology and the Intelligence Subcommittee on Cybersecurity, we will continue to monitor this situation. We look forward to working on legislation to keep the Treasury Department, the Federal Reserve System, and all members of the banking sector safe from cyber threats. We request that you brief us on the work that the Treasury Department is doing to partner with the private sector to deter, mitigate, and eliminate cybersecurity threats posed by malicious actors, including nation-state adversaries.

Sincerely,

  
Robin L. Kelly  
Member of Congress

  
James A. Himes  
Member of Congress



National Security Archive,  
Suite 701, Gelman Library, The George Washington University,  
2130 H Street, NW, Washington, D.C., 20037,  
Phone: 202/994-7000, Fax: 202/994-7005, [nsarchiv@gwu.edu](mailto:nsarchiv@gwu.edu)