COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Subcommittee Hearing Statement of Ranking Member Bennie G. Thompson (D-MS)

Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland

January 13, 2026

I appreciate the opportunity to discuss opportunities to disrupt and deter malicious cyber activities on domestic networks and impose costs on our adversaries, and I thank the witnesses for participating.

Before I begin, however, I would like to send my deepest condolences to the family of Renee Good, particularly her partner and six-year-old child, who is now without a mother. From everything I've seen, Ms. Good was attempting to de-escalate and leave the situation, and there was no reason to take her life. I support a full investigation of this shooting and justice on her behalf.

Turning to the issue at hand, over the course of the past year, there has been increased discussion about whether the United States is using its formidable offensive cyber capabilities as effectively as it could be to deter and disrupt cyber attacks. The United States' offensive cyber capability is second to none, – but with that awesome power comes awesome responsibility. As we consider whether and how to deploy offensive cyber tools differently, we must bear three points in mind:

First, cyber offense is no substitute for defense and resilience. We will have to continue investing in those key capabilities. Second, cyber offense is one tool among many – including sanctions and other diplomatic levers - that the United States can use to shape adversary behavior. The tool - or combinations of tools - we use should align with our mission objectives. And, finally, any significant change to our approach to the use of offensive cyber operations could shift global norms, and we must consult our allies.

As the Committee responsible for overseeing the Cybersecurity and Infrastructure Security Agency (CISA), I am concerned that we are putting the cart before the horse with a hearing on offensive cyber activity when we have not yet had a hearing on why the Agency has lost one-third of its workforce over the past year. CISA is the agency responsible for helping utilities, water treatment facilities, pipelines, and other critical infrastructure entities keep Volt Typhoon and other adversaries off their networks.

But ever since last January, the Trump administration harassed key CISA personnel into leaving their jobs, including the individuals responsible for the Secure by Design program, the Pre-Ransomware Notification Initiative, and individuals who worked directly with critical infrastructure operators on security issues.

We ought to be cautious about pursuing an approach involving the use of offensive cyber tools that could result in retaliation or escalation if we are not in a position to help defend U.S. networks. Moreover, we must bear in mind that offensive tools are one of many tools at our disposal to shape behavior in cyberspace – and we need to use them all more effectively and more deliberately. I understand that plans to impose sanctions on China's Ministry of State Security for its Salt Typhoon campaign were put on hold last year as the President negotiated a trade "truce" with the country.

Our use of sanctions and other diplomatic tools to deter and impose costs on our adversaries would be more effective if our President did not start unnecessary trade wars. Relatedly, we should be clear eyed about what our objectives are and how the use of offensive cyber tools aligns with those objectives.

Finally, any change in our approach to the use of offensive cyber tools that would shift current norms must be done in consultation with our allies. We cannot afford to distance ourselves from our security partners more than this administration already has. Having said all that, I agree there are opportunities to increase pressure and impose higher costs on adversaries for unacceptable behavior in cyberspace.

We should consider whether there are ways to more aggressively disrupt adversary infrastructure and deny them the benefits of success. Additionally, while offensive cyber activity is a government function, there may be new ways for the private sector to support government efforts in this space, in a manner consistent with the law.

# # #

Media contact