Issued 3/9/18

Cyber Threats are Coming at Us from All Sides.

In a highly anticipated speech on cyber security at Boston College, FBI Director Christopher A. Wray said Wednesday that the threat of digital warfare is “coming at us from all sides.” “We’re worried — at the FBI and with our partners — about a wider range of threat actors, from multi-national cyber syndicates and insider threats to hacktivists,” Wray said during a keynote address at the Boston Conference on Cyber Security on the BC campus. “And we’re concerned about a wider gamut of methods, from botnets to ransomware, from spearfishing and business e-mail compromise, to illicit cryptomining and APTs.” Wray cited an increase in state-sponsored cyber intrusions linked to North Korea and Russia as examples of the growing danger of such threats. “We’ve also begun seeing a ‘blended threat’ — nation-states using criminal hackers to do their dirty work,” Wray said, according to a transcript of his remarks. “Nation-state actors are also turning to more creative avenues to steal information. They are no longer dependent on just intelligence services to carry out their aims. Instead, they utilize people from all walks of life — hackers, businesspeople, academics, researchers, diplomats, tourists — and anyone else who can get their hands on something of value.” “We know that we need more cyber and digital literacy in every program throughout the Bureau — organized crime, crimes against children, white-collar crime, just to name a few,” he said. “We’re embedding noncyber agents with cyber squads, so they too can learn how to conduct cyber investigations. We’re sending noncyber personnel to cutting-edge cyber training. We’re also bringing intelligence analysts from the field to headquarters to get more tactical cyber experience. And we’re boosting our training for our most cyber-savvy agents, offering interactive, boot camp-type classes to walk agents through simulated cyber investigations.” A vanquished target of the FBI was

the Kelihos botnet, according to Wray. “Last year, the Kelihos botnet distributed hundreds of millions of fraudulent e-mails, stole banking credentials, and installed ransomware and other malicious software on computers all over the world,” he said. “We worked with our foreign law enforcement partners in both Spain and the Netherlands to identify and apprehend the Russian hacker and dismantle the botnet.” He urged companies to contact the bureau if they feel they’ve been targeted by hackers. “Please, when there are indications of unauthorized access to — or malware present on — critical IT systems, when an attack results in a significant loss of data, systems, or control of systems, when there’s a potential for impact to national security, economic security, or public health and safety, or when an intrusion affects critical infrastructure, call us,” Wray said.