https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537

COMMENTARY

It's Official: North Korea Is Behind WannaCry

The massive cyberattack cost billions and put lives at risk. Pyongyang will be held accountable.

Monitoring the WannaCry attack in South Korea, May 15. **PHOTO:** YUN DONG-JIN/ASSOCIATED PRESS

By Thomas P. Bossert
Dec. 18, 2017 7:15 p.m. ET

Cybersecurity isn't easy, but simple principles still apply. Accountability is one, cooperation another. They are the cornerstones of security and resilience in any society. In furtherance of both, and after careful investigation, the U.S. today publicly attributes the massive "WannaCry" cyberattack to North Korea.

The attack spread indiscriminately across the world in May. It encrypted and rendered useless hundreds of thousands of computers in hospitals, schools, businesses and homes. While victims received ransom demands, paying did not unlock their computers. It was cowardly, costly and careless. The attack was widespread and cost billions, and North Korea is directly responsible.

We do not make this allegation lightly. It is based on evidence. We are not alone with our findings, either. Other governments and private companies agree. The United Kingdom attributes the attack to North Korea, and Microsoft traced the attack to cyber affiliates of the North Korean government.

The consequences and repercussions of WannaCry were beyond economic. The malicious software hit computers in the U.K.'s health-care sector particularly hard, compromising systems that perform critical work. These disruptions put lives at risk.

The world is increasingly interconnected with new technologies, devices, networks and systems creating great convenience. Unfortunately, that provides bad actors opportunities to create mayhem with the hope of anonymity, relying on the complex world of ones and zeros to hide their hand. They have stolen intellectual property and done significant damage in every sector.

North Korea has acted especially badly, largely unchecked, for more than a decade, and its malicious behavior is growing more egregious. WannaCry was indiscriminately reckless.

Stopping malicious behavior like this starts with accountability. It also requires governments and businesses to cooperate to mitigate cyber risk and increase the cost to hackers. The U.S. must lead this effort, rallying allies and responsible tech companies throughout the free world to increase the security and resilience of the internet.

Change has started at the White House. President Trump has made his expectations clear. He has ordered the modernization of government information-technology to enhance the security of the systems we run on behalf of the American people. He continued sanctions on Russian hackers and directed the most transparent and effective government effort in the world to find and share vulnerabilities in important software. We share almost all the vulnerabilities we find with developers, allowing them to create patches. Even the American Civil Liberties Union praised him for that. He has asked that we improve our efforts to share intrusion evidence with hacking targets, from individual Americans to big businesses. And there is more to come.

As we make the internet safer, we will continue to hold accountable those who harm or threaten us, whether they act alone or on behalf of criminal organizations or hostile nations. Malicious hackers belong in prison, and totalitarian governments should pay a price for their actions. The rest of us must redouble our efforts to improve our collective defenses. The tool kits of totalitarian regimes are too threatening to ignore.

When we must, the U.S. will act alone to impose costs and consequences for cyber malfeasance. This year, the Trump administration ordered the removal of all Kaspersky software from government systems. A company that could bring data back to Russia represents an unacceptable risk on federal networks. Major companies and retailers followed suit. We brought charges against Iranian hackers who hacked several U.S. companies, including HBO. If those hackers travel, we will arrest them and bring them to justice. We also indicted Russian hackers and a Canadian acting in concert with them. A few weeks ago, we charged three Chinese nationals for hacking, theft of trade secrets and identity theft. There will almost certainly be more indictments to come.

Going forward, we must call out bad behavior, including that of the corrupt regime in Tehran. Whenever possible, we will work with partners, industry and allied governments, who share our market based values. We will rally our allies, and we will ensure the U.S. is again the leader in securing the internet we invented.

We call on the private sector to increase its accountability in the cyber realm by taking actions that deny North Korea and other bad actors the ability to launch reckless and destructive cyberattacks. We applaud Microsoft and others for acting on their own initiative last week, without any direction or participation by the U.S., to disrupt the activities of North Korean hackers.

As for North Korea, it continues to threaten America, Europe and the rest of the world—and not just with its nuclear aspirations. It is increasingly using cyberattacks to fund its reckless behavior and cause disruption across the world. Mr. Trump has already pulled many levers of pressure to address North Korea's unacceptable nuclear and missile developments, and we will continue to use our maximum pressure strategy to curb Pyongyang's ability to mount attacks, cyber or otherwise.

Mr. Bossert is assistant to the president for homeland security and counterterrorism.