2011: The year of cyber

A look back at a year when cyberattacks and responses reached a new level

BY JOHN EDWARDS

Future historians may conclude that 2011 marked a time when military cyber threats reached a tipping point, transforming a once mostly theoretical menace into an entirely new warfare domain.

Following in the footsteps of Stuxnet, elusive hackers in 2011 stepped up their attacks on military and intelligence assets. Meanwhile, the Defense Department introduced a new strategy aimed at dealing with existing and future cyber threats. The year now ending also saw cyber commands across all services step up the deployment of personnel, systems and other resources in a coordinated effort to defend military and contractor assets against cyberattacks originating at home and abroad.

Cedric Leighton, a retired Air Force colonel who until 2010 was deputy director for training at the National Security Agency said this year's overarching theme was the emergence of increasingly sophisticated cyberattacks linked to suspected state actors. "China is the most-mentioned culprit, but Russia and others [also] have significant cyberwarfare capabilities," said Leighton, who now runs a Washington-based strategic risk consulting firm. Despite the growing number of cyber commands, Leighton said DOD needs to do more to protect vulnerable assets. "U.S defenses may be adequate in a few areas, but overall they and associated cyber strategies are not keeping pace with the threat," he said.

In July, DOD unveiled its long awaited cyber strategy comprised of five initiatives designed to provide a framework for military offensive and defensive operations in cyber space. "It did officially classify cyber as a separate operational domain of warfare, similar to air, sea and land, but [it] fell woefully short of being a true strategy because it focused mainly on defensive actions and did not adequately address offensive options as a military strategy document should," Leighton said.

Also in July, outgoing Deputy Secretary of Defense William Lynn revealed that 24,000 sensitive files on defense contractors' systems had been compromised. "The deputy secretary declared that an unnamed nation state was behind the data compromise," Leighton said. "Most experts suspected China was that country."

Of all the cyberattacks in 2011, the most potentially damaging one occurred in March when hackers raided EMC's RSA division and data pertaining to RSA's SecurID tokens. "This [attack] apparently played a role in the subsequent hacking of defense contractors Lockheed Martin, Northrop Grumman, L-3 and perhaps others," said David Smith a senior fellow at the Potomac Institute for Policy Studies, a Washington-based technology and security think tank. "The M.O. suggests China as the origin of the cyber heist, but exactly who did it, what they were after and what they got is not publicly known," said Smith, a retired Air Force major who led U.S. negotiators in defense and space talks with the Soviet Union in the early 1990s. "One prominent analyst suggested they might have been seeking plans for the new Department of Homeland Security headquarters building," Smith said.

Although Stuxnet's existence was publicly revealed in 2010, reverberations were felt through 2011. "The analysis of exactly what it did, perhaps to Iranian nuclear reactors, and who authored it, continues," Smith said. "Then, late in 2011, the Duqu Worm was discovered, and some believe that it is related to Stuxnet."

Like Stuxnet, WikiLeaks' effects echoed across 2011. "This was the result of a low-tech human worm — allegedly, secret cables were downloaded onto a CD from which Lady Gaga had been erased," Smith says. "As Britain appears set to send Julian Assange back to Sweden to face allegations of rape, there are plenty of strings on which to pull in the WikiLeaks case, but the big lesson is that the human in the loop is the weakest link of any security system." ■

A student trains at the Defense Cyber Investigations Training Academy. In 2011, cyber commands across all services stepped up efforts to defend military and contractor assets against a steady stream of cyberattacks.