The National Guard takes on hackers

January 30 2014

At home, the National Guard is summoned during natural disasters and civil unrest. Overseas, it complements the active duty military. Now, the nation's governors want to mobilize the Guard to take on a new threat: cyberattacks.

Terrorists could endanger thousands or even millions of Americans by crippling the computer infrastructure of water utilities or the electrical grid. Meanwhile, criminals are anxious to get their hands on the financial, medical and other personal data states hold in their electronic records.

Guard units in every state have made great strides in protecting their own computer infrastructure, and governors say the Guard is well-equipped to meet broader state demands for cybersecurity.

In an October 2012 survey of states' chief information security officers, 70 percent of them said their state had experienced a cybersecurity breach. Only 24 percent said they felt "very confident" that their state assets were protected against external threats, and only 32 percent said their staffs were competent to protect against cyberattacks.

Colorado Gov. John Hickenlooper, who is the vice chairman of the National Governors Association, addressed the issue during the annual "State of the States" speech earlier this month in Washington, D.C.

"As the nation develops resiliency to cyberattacks, the Guard should be mobilized to support federal and state efforts to protect networks and

respond to incidents," said Hickenlooper, a Democrat. "While the federal government seeks to clarify how it will work with the private sector and states to better secure cyberspace, states are already moving forward to develop and implement new cyberpolicies to protect their economies and ensure public safety."

The federal government is taking notice, judging from the National Defense Authorization Act President Barack Obama signed into law on Dec. 26. The measure requires the Department of Defense to consider the Guard's capabilities as it shores up the Pentagon's cybersecurity. It also orders the department to consult with governors as it assesses states' cybersecurity needs and the Guard's ability to help on that front.

Furthermore, last March eight U.S. senators introduced a bill to establish "cybersecurity civil support teams" in the National Guard, similar to Guard teams that have been created to deal with incidents involving weapons of mass destruction. Under the measure, a governor or the secretary of defense could activate the teams in response to a cyberattack.

"The Cyber Warrior Act will ensure that in the first hours and days after a devastating cyberattack, our local responders will have the same support of the National Guard for response and recovery that they do when a hurricane strikes," said Democratic Sen. Christopher Coons of Delaware, a co-sponsor of the measure.

Washington was the first state to find a role for the National Guard in its cybersecurity efforts, said Maj. Gen. Tim Lowenberg, who commanded the state's forces as adjutant general from 1999 to 2012 before retiring from the Guard, and is now vice president of Gordon Thomas Honeywell Governmental Affairs. Missouri, Maryland, Delaware, Utah, and Rhode Island are among the other states that have created Guard units to counter cyberattacks.

Guard soldiers hold civilian jobs or attend college while maintaining their military training part time. Washington recognized the potential of its Guard as a cyberforce when it discovered that many of its Guard soldiers spent the workweek toiling for tech-related employers such as Google, Boeing, Northrop Grumman, Comcast, Verizon, Microsoft, Cisco and Hewlett-Packard. Washington decided to capitalize on that experience.

"It is generally accepted that we will never be able to recruit, train and retain sufficient numbers of (active duty) cybersecurity specialists in the military to meet our national security requirements," Lowenberg said. "With the National Guard, we found a combination of leading-edge technical knowledge and long and stable career commitment that are really unique."

Washington has used its Guard for cyberemergency planning and to search for vulnerabilities in its state networks through "red team" exercises conducted at the direction of the governor. Such exercises were used to demonstrate the security of the Washington Department of Licensing's network when the state was seeking permission to implement an Enhanced Driver License, which can be used to cross the Canadian border, according to Lowenberg. Implementing the program required persuading the U.S. Department of Homeland Security to allow access to its databases - which required hard proof of network security.

Lowenberg said the result of the National Guard's efforts in Washington state is a higher level of security - and a higher level of preparedness if an attack on critical infrastructure proves unavoidable.

"This would not be a pick-up game," he said. "We've fully developed the responses and protocols for all of this."

Another advantage to using the Guard, according to the National Guard

Association of the United States, is that Guard soldiers come from the communities they serve, giving them knowledge of state and local infrastructure that is difficult for federal officials to replicate.

"The National Guard provides a cost-effective and uniquely capable force that can provide capability for the DoD, homeland defense, civil support and intrastate missions," the group said in a statement. "Most importantly, the National Guard is composed of citizen-soldiers, working in communities and providing knowledge of critical infrastructure at the local level."

Heather Hogsett of the National Governors Association echoed that view.

"You don't necessarily know where a cyberattack is coming from, but it has a very localized impact," Hogsett said, adding that the Guard is accustomed to serving in a wide variety of roles under governors' direction.