Nation's fight against cyber intruders goes local

July 20 2011, By LAURA CRIMALDI , Associated Press

The next frontier in the fight to keep crucial electronic networks safe from harm will play out as close to home as Town Hall and require more involvement from private industry, which controls 85 percent of the infrastructure, experts say.

An explosion in threats against the nation's cyber networks has led the Pentagon to develop a cyber war strategy and states to open cyber security offices.

The Pentagon revealed last week that it sustained, earlier this year, one of its largest-ever losses of sensitive data in a cyberattack by an unnamed foreign government. Deputy Secretary of Defense William Lynch disclosed the theft of 24,000 files while outlining the military's new cyber war strategy.

"What keeps me up at night is just that we have so much more work to do," said Michael Kaiser, executive director of the National Cyber Security Alliance. "We have to figure out how to work together or we'll never achieve cyber security."

At his confirmation hearing last month, Secretary of Defense Leon Panetta told senators America's next great battle will likely entail cyber warfare.

"The next Pearl Harbor we confront could very well be a cyberattack that cripples our power systems, our grid, our security systems, our

financial systems, our governmental systems," Panetta said. He has said that cyber security will be a key focus of his Pentagon tenure.

A report by Verizon, the U.S. Secret Service and Dutch High Tech Crime Unit found the number of records compromised in data breaches fell to 4 million last year from 144 million in 2009 and a whopping 361 million in 2008.

The report's authors say the decline in data loss is tied to a decrease in large-scale data breaches.

Cyber security giant Symantec says it recorded more than 3 billion malware attacks last year.

The Federal Bureau of Investigation on Tuesday arrested 14 people in nine states and the District of Columbia on charges out of California that they hacked into PayPal's web site last December as part of the group "Anonymous," according to the U.S. Department of Justice.

Investigators say the hackers targeted PayPal after the online service suspended WikiLeak's account in the wake of the release of classified U.S. State Department cables. Prosecutors allege the cyberattack unleashed by the "Anonymous" group rendered PayPal inaccessible for users. They say the group dubbed the assault "Operation Avenge Assange," a reference to WikiLeaks founder Julian Assange.

Other recent high-profile victims of cyberattacks include the Massachusetts Institute of Technology, Sony, Citigroup, the International Monetary Fund, the Gmail accounts of high-ranking U.S. officials and the computer security company RSA, which sells devices used to protect computer systems. Also lurking are computer viruses and worms that have the potential to overtake systems controlling pipelines, water systems, nuclear power plants and other facilities.

Rhode Island officials highlighted the need for cooperation from the private sector when it unveiled its new Cyber Disruption Team. The July 11 announcement took place at the Providence offices of Dell SecureWorks, which services customers in the financial services, utilities, health care, retail and government industries. The team, with representatives from law enforcement, academia and Dell SecureWorks, aims to prevent and respond to cyber security events and defend the state's cyber infrastructure.

"That public-private partnership is absolutely critical," said U.S. Rep. Jim Langevin, D-RI, who is co-founder of the Congressional Cybersecurity Caucus.

At the same time, combatting cyber security is getting more local, Kaiser said. The Washtenaw County Cyber Citizenship Coalition in Michigan and Cyber City USA in San Antonio, Texas are two such examples.

"Local is actually the next frontier," Kaiser said. "People turn first to their local government, law enforcement, fire departments, town council, local mayor. We need them to be prepared and ready."

States began taking cyber security seriously while also fortifying physical targets after the Sept. 11 attacks, said George Foresman, a former undersecretary at the U.S. Department of Homeland Security. He said implementing cyber security measures has not been as consistent as the roll-out of homeland security efforts.

"It is still very much inconsistent and within that inconsistency lies a lot of vulnerabilities for states," Foresman said. States including Georgia, New York and California run cyber security offices to protect state networks.

In New York, the 40-person staff at the state's Office of Cyber Security

annually processes 26 billion pieces of data culled from Internet monitoring devices, said director Thomas D. Smith. More than 150 events require immediate attention every year and the office's Incident Response Team typically investigates more than 50 cyber incidents annually, Smith said. Last year, New York's disaster preparedness statute was also amended to include "cyber events" as grounds for declaring a state of disaster emergency, Smith said.

The workload, however, is a fraction of what the private sector manages because it controls a larger percentage of cyber networks.

In announcing the Rhode Island Cyber Disruption Team, Maj. Alan J. White, who is Dell SecureWorks's director of security and risk consulting and leader of the Rhode Island Army National Guard's Computer Emergency Response Team, said the company processes about 15 billion cyber security events daily to protect its customers.

"It's usually the government that wants something done about these attacks but the infrastructure is usually owned by the private enterprise," said Shari L. Pfleeger, director of research at the Institute for Information Infrastructure Protection at Dartmouth College. "You can't only do government. They are so intertwined. They are so interconnected. There needs to be a more comprehensive approach."

Yacov Y. Haimes, director of the Center for Risk Management of Engineering Systems at the University of Virginia, said because private and public cyber networks are so closely linked he supports federal legislation that proposes to create a gold standard for cyber defense that can be applied to privately-run networks.

The bill, crafted by U.S. Sens. Joe Lieberman I-Conn., Susan Collins, R-Maine, and Tom Carper, D-Del., would create a National Center for Cybersecurity and Communications with authority to direct federal

efforts to secure the cyber networks of government and the private sector.

One provision of the legislation would offer liability protection to network owners and operators of crucial infrastructure like electric grids and power plants who stick to security plans with a government seal of approval.

"The private sector is not ready to invest in the proper security because it's coming from the bottom line," Haimes said.

J. David Smith, former executive director of the RI Emergency Management Agency, said cooperation from the private sector is crucial not just to improve security on public networks, but to find more funding streams. The Rhode Island effort has financial support from the state police and emergency management officials, but no money has been set aside explicitly for the Cyber Disruption Team.

The scope of the task ahead is also daunting. New York is asking agencies to identify where sensitive information and data are stored, such as smart phones, laptops and computers, Smith said. He described the effort as a priority because it's impossible to protect data until establishing where it's stored. But the state has not imposed a deadline for agencies to report back because tight budgets have depleted manpower so dramatically.

Meanwhile cyber intruders are stepping up their game.

"We're seeing increasing sophistication in the way that hackers debilitate systems," Kaiser said. "There's still a lot of work to do."