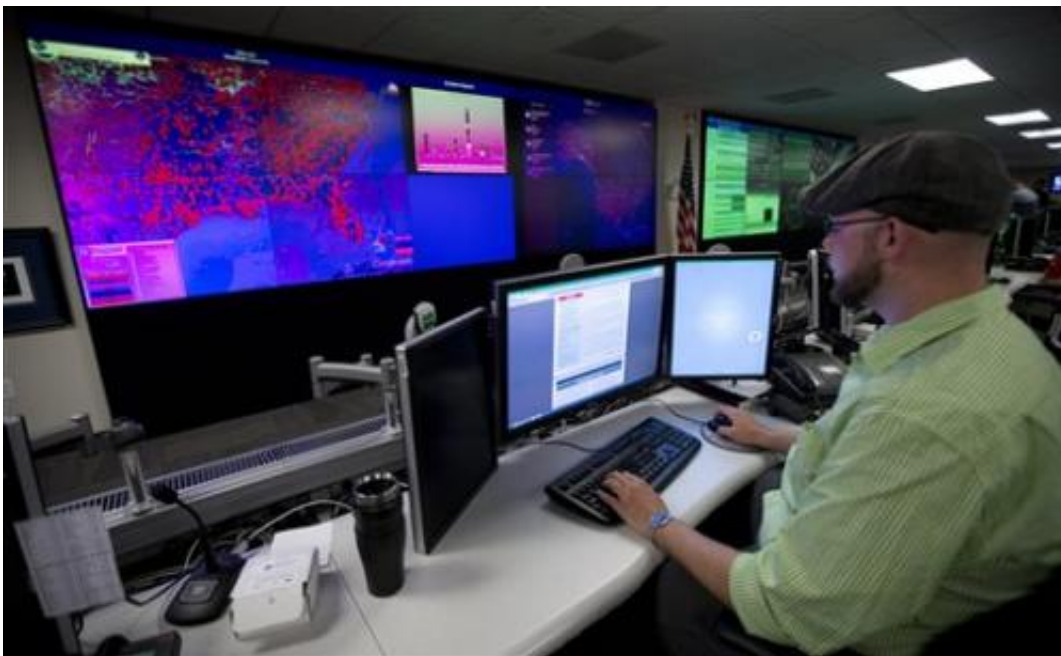# US fights cybercrime from suburban office parks

November 11 2014, by Martha Mendoza

A specialist works at the National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, Va., Tuesday, Sept. 9, 2014. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. Only after passing a low-key receptionist stationed on the seventh floor does one see the metal detectors, personal cellphone lockers and a series of heavy doors marked "classified" _ all leading to the auditorium-sized National Cybersecurity and Communications Integration Center. (AP Photo/Manuel Balce Ceneta)

Ground zero in the nation's fight against cybercrime hides in plain sight,

in a nondescript suburban office building with no government seals or signs.

Only after passing a low-key receptionist stationed on the seventh floor does one see the metal detectors, personal cellphone lockers and a series of heavy doors marked "classified"—all leading to the auditorium-sized National Cybersecurity and Communications Integration Center.

Inside, close to 100 specialists monitor floor-to-ceiling maps of the U.S. and world, along with streams of data and breaking news.

"This is where we put out the fires," says Phyllis Schneck, chief cybersecurity official for the Department of Homeland Security, nodding at an image of a rotating globe on a monitor the size of a movie screen.

This fall, The Associated Press paid rare visits to two key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists.

Cyberattack now eclipses terrorism as the biggest threat to national security, according to U.S. intelligence chiefs. And an AP report published this week found the $10 billion-a-year federal effort to protect the nation online is failing to keep up with attackers.

The hubs for the nation's online defense are tucked away in office parks mostly in Washington's sprawling suburbs. There are no external signs these are classified facilities. The AP was granted access only after agreeing to not disclose the locations and other identifying information.

Specialists work at the National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, Va., Tuesday, Sept. 9, 2014. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. Only after passing a low-key receptionist stationed on the seventh floor does one see the metal detectors, personal cellphone lockers and a series of heavy doors marked "classified" _ all leading to the auditorium-sized National Cybersecurity and Communications Integration Center. (AP Photo/Manuel Balce Ceneta)

Inside the DHS cybersecurity center, rows of industry, military and intelligence analysts watch three large monitors on each of their desks; they're detecting, preventing, responding to and mitigating cyberattacks.

Some scan through columns of numbers, monitoring live data fed through the federal "Einstein" program, a software system that searches

government networks for malware, viruses and hacks. Others spot defaced websites and data leaks. Frequently, teams travel directly to infected computers to get them off the network.

Department of Homeland Security spokesman Sy Lee declined to comment on whether the center was involved in stopping a recently reported cyberattack on White House networks, but he said DHS generally leads such response efforts.

At the Defense Cyber Crime Center cybercrime soldiers and defense contractors extract information from devices seized from battlefields, military crime scenes and federal employees whose computers may have been hacked.

Specialists work at the National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, Va., Tuesday, Sept. 9, 2014. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. Only after passing a low-key receptionist stationed on the seventh floor does one see the metal detectors,

personal cellphone lockers and a series of heavy doors marked "classified" _ all leading to the auditorium-sized National Cybersecurity and Communications Integration Center. (AP Photo/Manuel Balce Ceneta)

They crack encryption on devices, unlock cellphones and disassemble laptops.

The specialists don't hit an "on" switch until the equipment is placed inside a sealed box, to prevent Wi-Fi signals from reaching or being sent from the devices. A technician with a magnifying glasses leans over a digital tablet's colorful circuit board, soldering small wires that could eventually allow him to peek into the user's emails, documents and web-browsing habits.

Specialists like him are in high demand, as private sector cybersecurity jobs can pay double federal salaries, which average around $80,000 a year. The Defense Department this year announced plans to triple its cyberwarrior force to 6,000 by the end of 2016, and the Justice Department is also recruiting hundreds of cyber-savvy contractors and civil servants.

Hard drives with bullet holes are displayed at the Defense Computer Forensics Laboratory (DCFL), Wednesday, Sept. 10, 2014, in Linthicum, Md. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. This fall, The Associated Press paid rare visits to key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists. (AP Photo/Manuel Balce Ceneta)

A specialist solders a piece of wire to a mother board that will be attached to a computer to collect information at the Defense Computer Forensics Laboratory (DCFL), in Linthicum, Md., Wednesday, Sept. 10, 2014. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. This fall, The Associated Press paid rare visits to key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists. (AP Photo/Manuel Balce Ceneta)

A specialist hold a hard drive seized during the Gulf War, at the Defense Computer Forensics Laboratory (DCFL), Wednesday, Sept. 10, 2014, in Linthicum, Md. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. This fall, The Associated Press paid rare visits to key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists. (AP Photo/Manuel Balce Ceneta)
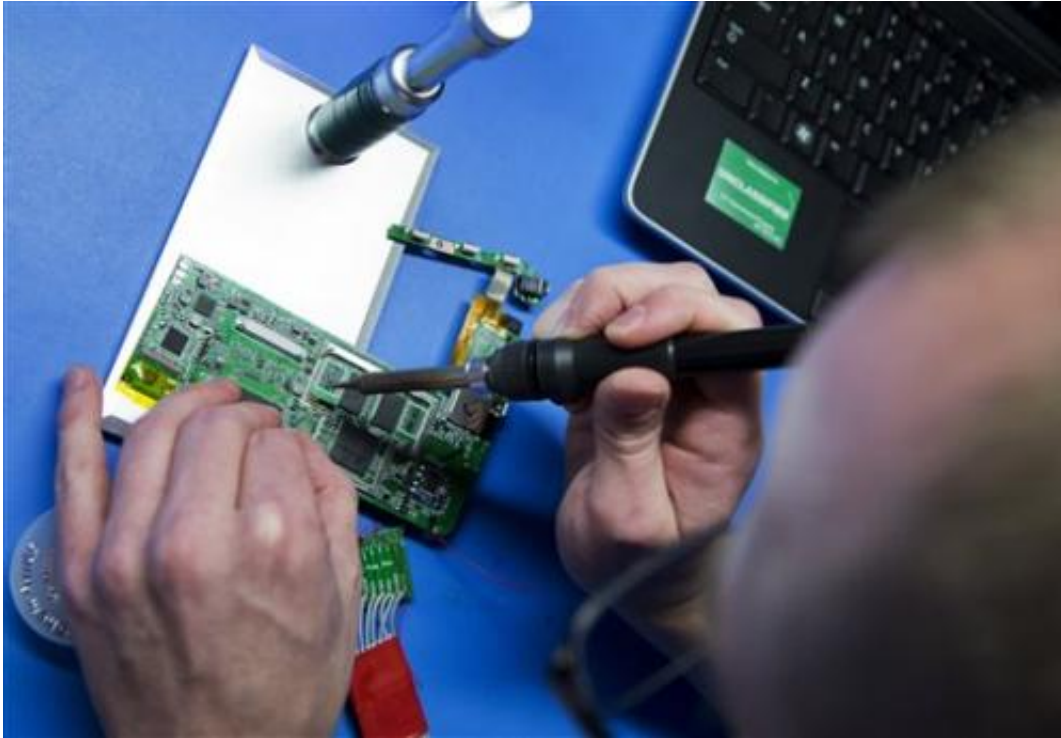
Evidence items are displayed t the Defense Computer Forensics Laboratory (DCFL), Wednesday, Sept. 10, 2014, in Linthicum, Md. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. This fall, The Associated Press paid rare visits to key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists. (AP Photo/Manuel Balce Ceneta)

Evidence items are displayed at the Defense Computer Forensics Laboratory (DCFL), Wednesday, Sept. 10, 2014, in Linthicum, Md. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. This fall, The Associated Press paid rare visits to key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists. (AP Photo/Manuel Balce Ceneta)
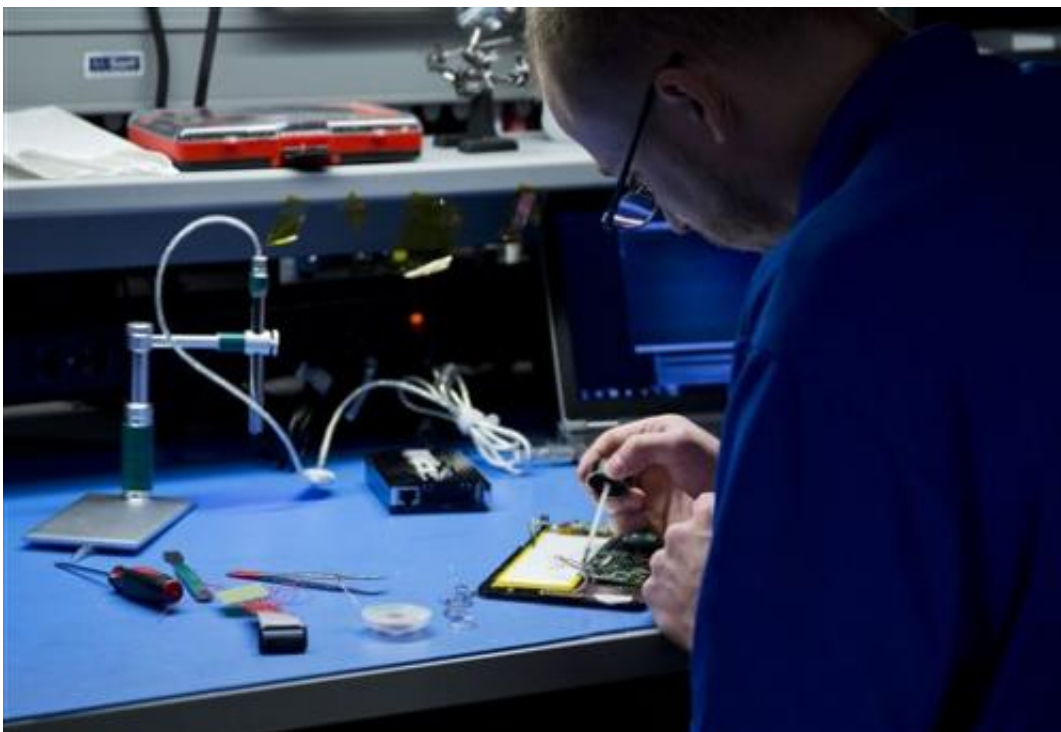
A specialist works at the Defense Computer Forensics Laboratory (DCFL), Wednesday, Sept. 10, 2014, in Linthicum, Md. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. This fall, The Associated Press paid rare visits to key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists. (AP Photo/Manuel Balce Ceneta)

A specialist works at the National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, Va., Tuesday, Sept. 9, 2014. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. Only after passing a low-key receptionist stationed on the seventh floor does one see the metal detectors, personal cellphone lockers and a series of heavy doors marked "classified" _ all leading to the auditorium-sized National Cybersecurity and Communications Integration Center. (AP Photo/Manuel Balce Ceneta)

A specialist solders a piece of wire to a mother board that will be attached to a computer to collect information at the Defense Computer Forensics Laboratory (DCFL), in Linthicum, Md., Wednesday, Sept. 10, 2014. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. This fall, The Associated Press paid rare visits to key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists. (AP Photo/Manuel Balce Ceneta)

A specialist solders a piece of wire to a mother board that will be attached to a computer to collect information at the Defense Computer Forensics Laboratory (DCFL), in Linthicum, Md., Wednesday, Sept. 10, 2014. Ground zero in the nation's fight against cybercrime hides in plain sight, in a nondescript suburban office building with no government seals or signs. This fall, The Associated Press paid rare visits to key civilian and military cybersecurity centers, a secret lab and a 24/7 incident-response venue where the government's computer scientists work to combat an increasing bombardment by thieves, hostile states and hacktivists. (AP Photo/Manuel Balce Ceneta)

Citation: US fights cybercrime from suburban office parks (2014, November 11) retrieved 23 April 2024 from https://phys.org/news/2014-11-cybercrime-suburban-office.html