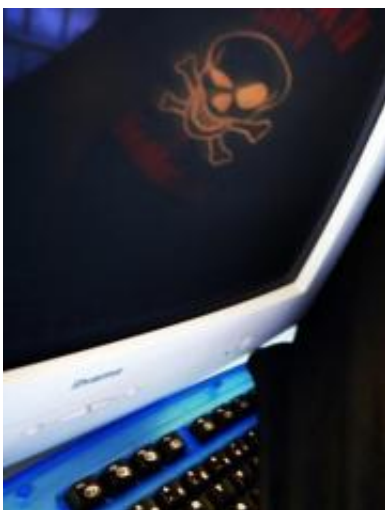# Elite US cyber team courts hackers to fight terror

August 2 2010, by Glenn Chapman

Skull and crossbones reflected in a computer screen. An elite US cyber team that has stealthily tracked Internet villains for more that a decade pulled back its cloak of secrecy to recruit hackers at a notorious DefCon gathering here Sunday.

An elite US cyber team that has stealthily tracked Internet villains for more than a decade pulled back its cloak of secrecy to recruit hackers at a DefCon gathering.

Vigilant was described by its chief Chet Uber as a sort of cyber "A-Team" taking on terrorists, drug cartels, mobsters and other enemies on the Internet.

"We do things the government can't," Uber said on Sunday. "This was never supposed to have been a public thing."

Vigilant is an alliance of slightly more than 600 volunteers and its secret ranks reportedly include chiefs of technology at top firms and former high-ranking US cyber spies.

The group scours [Internet traffic](#) for clues about online attacks, terrorists, cartels and other targets rated as priorities by members of the democratically run private organization.

Vigilant also claimed to have "collection officers" in 22 countries that gather intelligence or coordinate networks in person.

"We go into bars, look for lists of bad actors, get tips from people..." Uber said.

"But, a significant amount of our intelligence comes from our monitoring the Internet. We are looking at everything on websites, and websites are public."

He was adamant that Vigilant stays within US law while being more technologically nimble than government agencies weighed down by bureaucracy and internal rivalries.

"Intelligence is a by-product of what our research is," Uber said. "Our research is into attacks, why they happen and how we can prevent them."

Vigilant shares seemingly significant findings with US spy agencies, and is so respected by leading members of the [hacker](#) community that Uber was invited to DefCon to recruit new talent.

Uber said that Vigilant came up from underground after 14 years of

operation in a drive to be at "full capacity" by adding 1,750 "vetted volunteers" by the year 2012.

"We are good people not out to hurt anybody," Uber said. "Our one oath is to defend the US Constitution against all enemies foreign and domestic."

Anything that can be looked at legally on the Internet is fair game for Vigilant, with email and encrypted transactions such as online shopping off limits.

The holy grail for Vigilant is finding out who is behind cyber attacks. Inability to figure out who launches online assaults routinely leaves companies or governments without targets to fire back at.

"This is a completely unsolved problem," Uber said. "We've probably been working on it as long as the government has."

Vigilant has developed its own "obfuscation" network to view "bad actors" on the Internet without being noticed.

He told of uncovering evidence of fraud in the latest presidential election in Iran while testing a way for people to slip information out of countries with oppressive regimes.

The information obtained was given to US officials.

"They expected fraud but they didn't expect the wholesale fraud that we passed along," Uber said.

Vigilant's network claimed a role relaying Twitter messages sent by Iranian protestors in the aftermath of the election.

The group is bent on gathering intelligence by any legal means and then putting the pieces together to see bigger pictures.

"The wholesale tapping of the Internet around the world can't be done," Uber said. "We are looking at what people write, how people attack, how attacks happen...we don't care who that person is."

Uber is working on a mathematical model to spot when terrorist organizations are recruiting teenagers online. The group has 100 projects in the works.

"Our end goal is to provide software as a service to government agencies so we can get out of the business of intelligence," Uber said.

Along with technology savants, Vigilant is recruiting sociologists, psychologists, and people with other specialties.

The wall between "feds" and hackers has been crumbling at DefCon, which has become a forum for alliances between government crime fighters and civilians considered digital-age "ninjas."

(c) 2010 AFP