INFILTRATION OF HACKER GROUPS

One in four US hackers 'is an FBI informer'

The FBI and US secret service have used the threat of prison to create an army of informers among online criminals

A quarter of hackers in the US have been recruited by federal authorities, according to Eric Corley, publisher of the hacker quarterly, 2600. Photograph: Getty Images

The underground world of computer hackers has been so thoroughly infiltrated in the US by the FBI and secret service that it is now riddled with paranoia and mistrust, with an estimated one in four hackers secretly informing on their peers, a Guardian investigation has established.

Cyber policing units have had such success in forcing online criminals to co-operate with their investigations through the threat of long prison sentences that they have managed to create an army of informants deep inside the hacking community.

In some cases, popular illegal forums used by cyber criminals as marketplaces for stolen identities and credit card numbers have been run by hacker turncoats acting as FBI moles. In others, undercover FBI agents posing as "carders" – hackers specialising in ID theft – have themselves taken over the management of crime forums, using the intelligence gathered to put dozens of people behind bars.

So ubiquitous has the FBI informant network become that Eric Corley, who publishes the hacker quarterly, 2600, has estimated that 25% of hackers in the US may have been recruited by the federal authorities to be their eyes and ears. "Owing to the harsh penalties involved and the relative inexperience with the law that many hackers have, they are rather susceptible to intimidation," Corley told the Guardian.

"It makes for very tense relationships," said John Young, who runs Cryptome, a website depository for secret documents along the lines of WikiLeaks. "There are dozens and dozens of hackers who have been shopped by people they thought they trusted."

The best-known example of the phenomenon is Adrian Lamo, a convicted hacker who turned informant on Bradley Manning, who is suspected of passing secret documents to WikiLeaks. Manning had entered into a prolonged instant messaging conversation with Lamo, whom he trusted and asked for advice. Lamo repaid that trust by promptly handing over the 23-year-old intelligence specialist to the military authorities. Manning has now been in custody for more than a year.

For acting as he did, Lamo has earned himself the sobriquet of Judas and the "world's most hated hacker", though he has insisted that he acted out of concern for those he believed could be harmed or even killed by the WikiLeaks publication of thousands of US diplomatic cables.

"Obviously it's been much worse for him but it's certainly been no picnic for me," Lamo has said. "He followed his conscience, and I followed mine."

The latest challenge for the FBI in terms of domestic US breaches are the anarchistic co-operatives of "hacktivists" that have launched several high-profile cyber-attacks in recent months designed to make a statement. In the most recent case a group calling itself Lulz Security launched an audacious raid on the FBI's own linked organisation InfraGard. The raid, which was a blatant two fingers up at the agency, was said to have been a response to news that the Pentagon was poised to declare foreign cyber-attacks an act of war.

Lulz Security shares qualities with the hacktivist group Anonymous that has launched attacks against companies including Visa and MasterCard as a protest against their decision to block donations to WikiLeaks. While Lulz Security is so recent a phenomenon that the FBI has yet to get a handle on it, Anonymous is already under pressure from the agency. There were raids on 40 addresses in the US and five in the UK in January, and a grand jury has been hearing evidence against the group in California at the start of a possible federal prosecution.

Kevin Poulsen, senior editor at Wired magazine, believes the collective is classically vulnerable to infiltration and disruption. "We have already begun to see Anonymous members attack each other and out each other's IP addresses. That's the first step towards being susceptible to the FBI."

Barrett Brown, who has acted as a spokesman for the otherwise secretive Anonymous, says it is fully aware of the FBI's interest. "The FBI are always there. They are always watching, always in the chatrooms. You don't know who is an informant and who isn't, and to that extent you are vulnerable."

Arrests of LulzSec and Anonymous members leads to claims that leader was an FBI informant

Four principal members of Anonymous and LulzSec have been charged with computer hacking, while two others have pleaded guilty to charges.

According to an FBI statement, the four have been charged in connection with the hacking of Fox Broadcasting Company, Sony Pictures Entertainment and the Public Broadcasting Service (PBS). Charges have also been made over the attacks on Fine Gael, a political party in Ireland, and on security firms HBGary and its affiliate HBGary Federal, and Stratfor.

Those charged have been named as Ryan Ackroyd (aka 'Kayla', 'Lolspoon'), Jake Davis (aka 'Topiary'), Darren Martyn (aka 'pwnsauce', 'raepsauce', 'networkkitten') and Donncha O'Cearrbhail (aka 'palladium'). O'Cearrbhail was also charged in a separate criminal complaint with intentionally disclosing an unlawfully intercepted wire communication.

A fifth member was named as Jeremy Hammond (aka 'Anarchaos', 'sup_g', 'burn', 'yohoho', 'POW', 'tylerknowsthis', 'crediblethreat'); he was charged with crimes relating to the December 2011 hack of Stratfor.

The sixth member was named as Hector Xavier Monsegur (aka 'Sabu', 'Xavier DeLeon', 'Leon'). However, the statement claimed that he pleaded guilty on 15 August in a US District Court to 12 counts of computer hacking conspiracies and other crimes, information that was unsealed today.

He had plead guilty to three counts of computer hacking conspiracy, five counts of computer hacking, one count of computer hacking in furtherance of fraud, one count of conspiracy to commit access device fraud, one count of conspiracy to commit bank fraud and one count of aggravated identity theft. He faces a maximum sentence of 124 years and six months in prison.

Jake Davis was arrested last year in the Shetland Islands on a charge of unauthorised computer access and conspiracy to carry out a distributed denial of service attack on the Serious Organised Crime Agency's (SOCA) website.

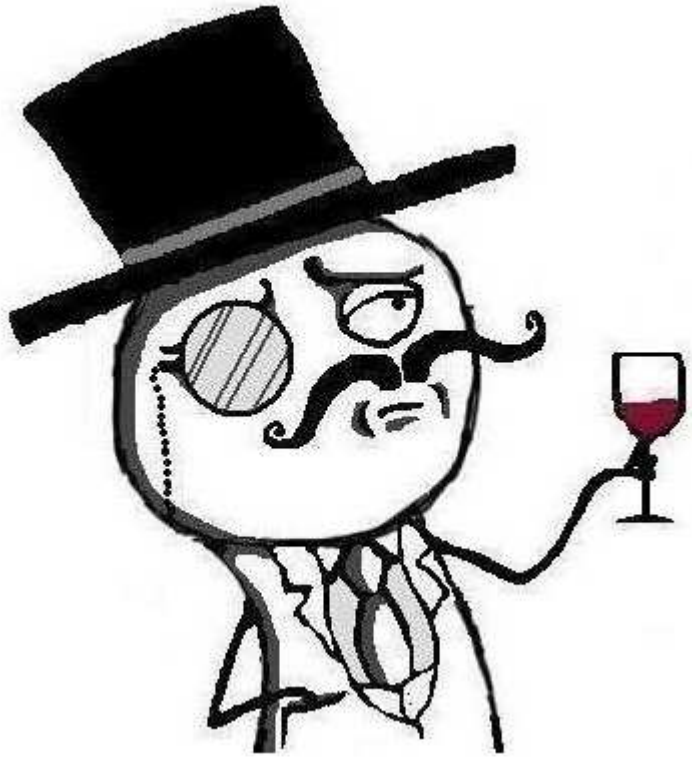
O'Cearrbhail was named as one of the two men arrested in connection with hacking of Fine Gael and was the son of Offaly County councillor John Carroll. He was later revealed to have been released without charge, along with another man.

A report by Fox News claimed that the arrests were largely made based on evidence gathered by Monsegur, with sources saying he has been secretly working for the US government for months. It claimed that working under the internet alias 'Sabu' and tweeting to more than 45,000 followers at Anonymousabu, the FBI unmasked him last June and he became a co-operating witness while commanding "a loosely organised, international team of perhaps thousands of hackers from his nerve centre in a public housing project on New York's Lower East Side".

“They caught him and he was secretly arrested and now works for the FBI,” a source close to Sabu told FoxNews.com.

Two hackers plead guilty to LulzSec attacks on Web sites

Ryan Cleary and Jake Davis, aka "Topiary," plead guilty to DDoS attacks; two others plead not guilty. The charges centered on events in a 50-day hacking spree last year.



The hacking group LulzSec, which derives from "Lulz" and Security, went on a 50-day hacking spree last year. Seven alleged members have been arrested and three have pleaded guilty.

(Credit: LulzSec)

Two British men pleaded guilty today to conspiracy charges related to a spree of attacks on U.S. and U.K. government and corporate Web sites by the LulzSec hacking group last year.

Ryan Cleary, 20, and Jake Davis, a 19-year-old who used the hacker handle "Topiary," admitted to launching distributed denial-of-service (DDoS) attacks on Web sites including Sony, Nintendo, News International, Arizona State Police, HBGary Federal and PBS, according to The Telegraph.

Cleary pleaded guilty to four additional charges, including hacking into U.S. Air Force computers at the Pentagon. He was indicted by a U.S. federal grand jury earlier this month on charges related to hacking into the Web sites of Fox, PBS and Sony Pictures. It is unclear if prosecutors in the U.S. will try to extradite Cleary to face those charges. His lawyer says she would fight extradition because her client has Asperger's Syndrome, according to The Associated Press.

Meanwhile Ryan Ackroyd, a 25-year-old who allegedly used the handle "Kayla," and a 17-year-old who was not named because of age but has been associated with the handle "T-Flow," pleaded not guilty to the conspiracy charges. They will face trial April 8, 2013, according to The Telegraph. All the defendants were released on bail, except for Cleary.

All four pleaded not guilty to two counts of encouraging or assisting others to commit computer offenses and fraud. They were accused of posting stolen data to public Web sites. Southwark Crown Court official Gryff Waldron told the AP that prosecutors are still deciding whether to bring Cleary and Davis to court on those charges.

The group is accused of stealing confidential information -- including passwords -- and releasing it publicly, hijacking e-mail accounts and even secretly listening in on a conference call in which the FBI and Scotland Yard talked about trying to catch them.

Davis, Ackroyd and T-Flow are believed to be three of the founders of LulzSec, along with the leader "Sabu," who was identified as Hector Xavier Monsegur by the U.S. Attorney's Office in New York in March. Monsegur had been arrested and released in June 2011 when he pleaded guilty and agreed to serve as informant. His cooperation resulted in the arrests of Ackroyd, Davis and others who were associated with Anonymous, but are not believed to have been core members of LulzSec, including Darren Martyn, also known as "pwnsauce," and Donncha O'Cearrbhail, aka "Palladium," both of Ireland.

Separately, Jeremy Hammond, aka "Anarchaos," was arrested in Chicago in March and charged with crimes related to the December 2011 hack of Stratfor, a global intelligence firm. He is not alleged to be a member of LulzSec.

Below is a timeline of major LulzSec events. Dates may be approximate as it is often difficult to determine exactly when a network was compromised:

February 2, 2011 - Anonymous hacks HBGary Federal site

May 15 - LulzSec claims credit for hacking UK ATMs and Fox Network's X Factor site

May 23 - LulzSec leaks data from Sony Music Japan

May 30 - LulzSec defaces PBS.org

June 2 - Group leaks customer data from Sony Pictures

June 3 - Hacks on Nintendo and InfraGard Atlanta

June 6 - Sony Entertainment source code and Sony BMG hacks

June 7 - Monsegur, aka Sabu, arrested on identity fraud charges

June 9 - LulzSec compromises U.K. National Health Services site

June 13 - Data stolen from videogame maker Bethesda Software

June 14 - Senate site compromised

June 15 - DDoS on CIA site

June 16 - Thousands of passwords dumped

June 20 - DDoS on U.K.'s Serious Organized Crime Agency

June 21 - British police arrest 19-year-old Ryan Cleary

June 23 - Arizona law enforcement sites compromised

June 25 - LulzSec announces that they are quitting after 50 days

June 28 - Zimbabwe, Brazil, UMG, Viacom hacked

June 29 - Arizona Dept. of Public Safety data dump

June 29 - FBI searches home of Ohio man

June 30 - another Arizona law officer data dump

July 4 - Apple server targeted

July 8 - Chilean government site, IRC Federal hacked

July 11 - hackers claim Booz Allen Hamilton hack

July 18 - LulzSec deface Murdoch's The Sun

July 19 - 16 arrested in U.S.

July 22 - U.S., Italian cyber crime site hacked

July 27 - Topiary arrested (Identified this week as Jake Davis)

August 6 - Italian police sites attacked

August 15 - Monsegur pleads guilty to computer hacking charges

August 18 - Hackers claim data stolen from Vanguard Defense Industries

September 22 - Arrest of Cody Andrew Kretsinger, 23, of Phoenix

December 25 - Stratfor data stolen

March 6 - AntiSec hacks Panda Security site to protest LulzSec arrests

June 13 - U.S. indicts Ryan Cleary for Fox, PBS hacks

Lulzer Sabu Turns in Top Anonymous Leadership

Fox News reports that infamous LulzSec leader known as Sabu has been working with law enforcement for months to investigate key members of the Anonymous movement, resulting in multiple arrests of key Anonymous conspirators.

"They caught him and he was secretly arrested and now works for the FBI," a source told Fox News.

Sabu, who has been identified as Hector Xavier Monsegur, a resident of New York, was apparently arrested and indicted back in August of 2011, and has been working with law enforcement to undermine the Anonymous movements top strategists, according to reports:

"On August 15, 2011 Monsegur pleaded guilty to more than ten charges relating to his hacking activity. In the following few weeks, he worked almost daily out of FBI offices, helping the feds identify and ultimately take down the other high-level members of LulzSec and Anonymous, sources said."

The arrests occurred in both Europe and the United States, and the list of suspects apprehended includes some of the most sought after hacktivists thought to be responsible for orchestrating attacks against multiple government and private sector targets.

"The five charged in the LulzSec conspiracy indictment expected to be unsealed were identified by sources as: Ryan Ackroyd, aka 'Kayla' and Jake Davis, aka 'Topiary,' both of London; Darren Martyn, aka 'pwnsauce' and Donncha O'Cearrbhail, aka 'palladium,' both of Ireland; and Jeremy Hammond aka 'Anarchaos,' of Chicago," reports noted.

Monsegur is said to have cooperated with the investigation out of concern for the welfare of his family, sources indicate.

"It was because of his kids. He didn't want to go away to prison and leave them. That's how we got him," a law enforcement official stated.

The law enforcement action could be a deathblow to the loosely organized collective known for their anti-government and anti-business antics, and more arrests are to be expected as the suspect's hardware is examined by forensics units.

"This is devastating to the organization. We're chopping off the head of LulzSec," said an unnamed FBI official.

Anonymous Spokesman 'Topiary' Arrested in Scotland

Breaking News:

"Scotland Yard says officers from its specialist cybercrime unit have arrested the suspected spokesman of the Lulz Security hacking group. In a statement Wednesday the police force says that the 19-year-old was arrested at an address in Scotland's Shetland Islands on Wednesday."

"They say he is the name behind the hacker known as 'Topiary,' who has given several interviews in recent weeks. As reported by ZDNet, Topiary is being transported from the Shetland Islands to a London police station and is expected to face charges related to cybercrime, network intrusions and hacking..."

Source: http://www.cbsnews.com/stories/2011/07/27/world/main20084221.shtml

*** * ***

Anonymous' PayPal Campaign Tempered by Arrests

The rogue hacktivist movement Anonymous has issued statements encouraging PayPal customers to close their accounts in protest of the company's decision to suspend fundraising accounts that benefit the international whistleblower organization WikiLeaks.

The new campaign is notably milder in nature than those in the past where the hacktivists organized a distributed denial of service (DDoS) attack against the company's publicly facing websites.

The less aggressive campaign may be due to apprehensions after fourteen individuals were arrested by FBI agents last week on charges related to their alleged involvement in the DDoS attack, though the Anonymous statements attempt to indicate otherwise.

On December 3rd, 2010 PayPal had announced it was suspending the fundraising accounts of WikiLeaks for violation of the Acceptable Use Policy, stating:

"PayPal has permanently restricted the account used by WikiLeaks due to a violation of the PayPal Acceptable Use Policy, which states that our payment service cannot be used for any activities that encourage, promote, facilitate or instruct others to engage in illegal activity. We have notified the account holder of this action. "

Following PayPal's suspension of the WikiLeaks account, Anonymous launched the DDoS attack, and tweeted the following messages:

"TANGO DOWN — thepaypalblog.com — Blog of Paypal, company that has restricted Wikileaks' access to funding. #Paypal #Wikileaks #WL #DDoS"

"Close your #Paypal accounts in light of the blatant misuse of power to partially disable #Wikileaks funding. Join in the #DDoS if you'd like"

The PayPal blog was reported to have been offline for several hours as a result. DDoS attacks are attempts to render web servers unavailable to users through a variety of means, including saturating the target networks with communications requests, thereby denying access to legitimate users.

Today's Pastebin announcement from Anonymous is as follows:

Dear PayPal, its customers, and our friends around the globe,

This is an official communiqué from Anonymous and Lulz Security in the name of AntiSec.

In recent weeks, we've found ourselves outraged at the FBI's willingness to arrest and threaten those who are involved in ethical, modern cyber operations. Law enforcement continues to push its ridiculous rules upon us - Anonymous "suspects" may face a fine of up to 500,000 USD with the addition of 15 years' jailtime, all for taking part in a historical activist movement. Many of the already-apprehended

Anons are being charged with taking part in DDoS attacks against corrupt and greedy organizations, such as PayPal.

What the FBI needs to learn is that there is a vast difference between adding one's voice to a chorus and digital sit-in with Low Orbit Ion Cannon, and controlling a large botnet of infected computers. And yet both of these are punishable with exactly the same fine and sentence.

In addition to this horrific law enforcement incompetence, PayPal continues to withhold funds from WikiLeaks, a beacon of truth in these dark times. By simply standing up for ourselves and uniting the people, PayPal still sees it fit to wash its hands of any blame, and instead encourages and assists law enforcement to hunt down participants in the AntiSec movement.

Quite simply, we, the people, are disgusted with these injustices. We will not sit down and let ourselves be trampled upon by any corporation or government. We are not scared of you, and that is something for you to be scared of. We are not the terrorists here: you are.

We encourage anyone using PayPal to immediately close their accounts and consider an alternative. The first step to being truly free is not putting one's trust into a company that freezes accounts when it feels like, or when it is pressured by the U.S. government. PayPal's willingness to fold to legislation should be proof enough that they don't deserve the customers they get. They do not deserve your business, and they do not deserve your respect.

Join us in our latest operation against PayPal - tweet pictures of your account closure, tell us on IRC, spread the word. Anonymous has become a powerful channel of information, and unlike the governments of the world, we are here to fight for you. Always.

Signed, your allies,

Lulz Security (unvanned)
Anonymous (unknown)
AntiSec (untouchable)

Is Anonymous' fervor being tempered by the recent arrests by federal law enforcement? We can only hope so.

Further arrests and indictments are expected as authorities continue their investigations into other Anonymous, LulzSec and AntiSec attacks, including those perpetrated against Visa, MasterCard, PostFinance Bank, Amazon, Bank of America, the U.S. Chamber of Commerce website, and for having breached the systems of security consultants HBGary Federal.

Was Anonymous-OS a government false flag operation?

By DJ Pangburn 105 days ago

When news broke that Anonymous had supposedly released a Linux-based operating system, Anonymous-OS, red flags began flapping in the wind.

Anonymous almost immediately advised internet users not to download the Ubuntu-based OS. YourAnonNews tweeted, "Seeing lots of news about just-released purported 'Anonymous OS.' BE CAREFUL! Remember the Zeus Trojan incident w/Slowloris recently!" A day later the OS was said to be riddled with malware.

The headline of this article is provocative, to be sure. But when I posed the question to a fellow D+T writer, the response was, "I've learned to never put anything past our government." At the very least we must entertain the possibility of a false flag operation following the FBI's infiltration of Antisec through Sabu.

Anonymous-OS, which comes loaded with hacking tools, was uploaded to Sourceforge and then downloaded over 26,000 times. Sourceforge took the OS down yesterday and issued an official statement:

"By taking an intentionally misleading name, this project has attempted to capitalize on the press surrounding a well-known movement in order to push downloads of a project that is less than a week old," said Sourceforge's spokesperson. "We have therefore decided to take this download offline and suspend this project until we have more information that might lead us to think differently. We'll be in touch with the project admin, and let you know if and when we find out anything to contrary, but for now, that's what we're doing."

Ars Technica's Sean Gallagher believes it's just a shoddily-designed variant of Ubuntu and, as such, not much of a worry unless the system is booby-trapped. That may well be the simple truth, but we might also consider the possibility that it was a bit of government-issued social engineering. That is, a false flag operation to paint Anonymous as malicious criminals who are more interested in corrupting personal computers than fighting economic, social or political injustice.

Consider the fact that the OS's supposed malware was being discussed soon after it was posted to Sourceforge. The chatter is significant because government spooks know what

advertisers, public relations gurus, or anyone with half a mind knows: to create a certain outcome, any message must be controlled and shaped at its inception. If you want to convince the public that Anonymous is not a digital protest movement but a "criminal" network, then you create the conditions to communicate that idea.

Anonymous can claim the OS was not their creation, and the OS itself might not be a real threat at all, but the symbolic association between Anonymous, the operating system, and malware has already bloomed in many people's minds.

As Graham Cluley of Sophos Naked Security wrote, "If I were writing a cybercrime thriller, I might dream up a plot where the computer cops – desperate to know the identities of the hacktivists – concocted a plot where they made available software that promised to hide hackers' identities.. but in fact secretly passed information back to the cops."

Cluley doesn't claim this is the case, but adds, "stranger things have happened.. (like the prominent leader of LulzSec turning out to have been secretly working for the FBI since the middle of last year..)."

In the final analysis, the truth may very well be that someone simply wanted to use the Anonymous name to publicize their Linux-based operating system, or deliver malware to dumb victims. I'm inclined to believe the former possibility myself, because infecting computers through a Linux-based OS (which is little known to the masses) isn't exactly the most efficient means of creating bad press for Anonymous.

Never put anything past our government, though.

Anonymous' new timeline of FBI infiltration suggests Antisec may have been an FBI creation

Today, the @YourAnonNews Twitter account theorized that Antisec, which was created just before LulzSec began retreating into Anonymous, was in fact the creation of the FBI.

At the time of Antisec's inception, there was some chatter within the hacking community that LulzSec created Antisec in order to stage some misdirection—to get authorities looking elsewhere. Almost simultaneously, if memory serves, some observers were even suggesting that government authorities, whether in the US or UK and elsewhere, were bearing down on LulzSec.

YourAnonNews has created a document laying out the timelines of the FBI's activity with Sabu and the rise of Antisec, and it's a very enlightening read.

For instance, the first mention of Antisec occurs on June 4, 2011, when The Lulz Boat Twitter feed tweets, “So gather round, this is a new cyber world and we’re starting it together. There will be bigger targets, there will be more ownage. #ANTISEC.” On June 7th, as we know, the FBI paid a visit to Sabu and got him singing arias.

On June 19th, Sabu returns from an extended break and tweets, “Operation Anti-Security:http://pastebin.com/9KyA0E5v – The biggest, unified operation amongst hackers in history. All factions welcome. We are one.” The same day Operation Antisec is announced via Pastebin.

Foreign "spy masters" could infiltrate hacker groups

Foreign powers could try to infiltrate hacktivist networks in order to manipulate their actions, according to a security expert who advises governments and businesses on internet issues.

The warning comes as governments and corporations - including defence manufacturers - come under widespread attack from hacker groups such as LulzSec and Anonymous, and amid growing fears about cyber espionage from sovereign powers, especially China.

Likening the emergence of the hacktivist movement to the arrival of militant groups such as the Red Brigade during the 1970s, government advisor and chair of the International E-crime Congress, Simon Moores, said that hacker groups could eventually be swayed by outside influences.

You could have the teenaged hacker who thinks they’re doing something for the greater good by revealing information or attacking greedy billionaires, but in fact they are being manipulated for more sinister purposes

“If you have a LulzSec or an Anonymous that is perhaps being manipulated by a foreign actor, it takes us back to the days of the Stasi and the KGB, which were manipulating [anti-nulear campaign group] CND quite easily from Moscow,” he said, referring to reports that the anti-nuclear peace movement was unwittingly compromised and manipulated by Kremlin machinations.

According to Moores, mustering popular support for an issue through online hacktivist groups and forums could be used as a tool to drive policy to perform actions that furthered a country's interests.

And because the hacker groups are distributed, anonymous and at least in part consist of ideologists – as shown with hacks against financial institutions when they blocked payments to WikiLeaks – Moores believed they were especially vulnerable to interference from outside sources.

“So you could have the teenaged hacker who thinks they’re doing something for the greater good by revealing information or attacking greedy billionaires, but in fact they are being manipulated for more sinister purposes by someone who has infiltrated their network,” he said. “If you were a spy master wouldn’t you be doing that?”

This just doesn't make sense…

let's take Lulzsec as an example.
Their 'power' comes from two places:
1- The knowledge and skill of a small group of people.
2 - The might and clout that comes with having a botnet or getting people to join in a DDOS attack. [this is what the person in the UK got caught doing]

So, if "foreign spy masters" have people with the skills to get in with a group like lulzsec, why don't they just get their own botnet and do what ever they want to do?
That's all lulzsec are. just a few people with the right knowledge and a botnet, anything they can do can be done by anybody with the same knowledge and resources.

If on the other hand they are talking about "anonymous" for example, then that's just laughable, anybody is free to join "anonymous" (you don't need to be a spy to get yourself into "anonymous") but the idea of anybody being able to sway the anarchic cross-hairs of anonymous onto a target of their choice is just absurd, it shows that the people who come up with this stuff don't know what they are talking about.

Anonymous' new timeline of FBI infiltration suggests Antisec may have been an FBI creation

Today, the @YourAnonNews Twitter account theorized that Antisec, which was created just before LulzSec began retreating into Anonymous, was in fact the creation of the FBI.

At the time of Antisec's inception, there was some chatter within the hacking community that LulzSec created Antisec in order to stage some misdirection—to get authorities looking elsewhere. Almost simultaneously, if memory serves, some observers were even suggesting that government authorities, whether in the US or UK and elsewhere, were bearing down on LulzSec.

YourAnonNews has created a document laying out the timelines of the FBI's activity with Sabu and the rise of Antisec, and it's a very enlightening read.

For instance, the first mention of Antisec occurs on June 4, 2011, when The Lulz Boat Twitter feed tweets, "So gather round, this is a new cyber world and we're starting it together. There will be bigger targets, there will be more ownage. **#ANTISEC**." On June 7th, as we know, the FBI paid a visit to Sabu and got him singing arias.

On June 19th, Sabu returns from an extended break and tweets, "Operation Anti-Security:http://pastebin.com/9KyA0E5v - The biggest, unified operation amongst hackers in history. All factions welcome. We are one." The same day Operation Antisec is announced via Pastebin.

In that statement, we find this paragraph:

> Welcome to Operation Anti-Security (#AntiSec) – we encourage any vessel, large or small, to open fire on any government or agency that crosses their path. We fully endorse the flaunting of the word "AntiSec" on any government website defacement or physical graffiti art. We encourage you to spread the word of AntiSec far and wide, for it will be remembered. To increase efforts, we are now teaming up with the Anonymous collective and all affiliated battleships.

If the FBI is ventriloquizing Sabu (which they were) at this time, then it would seem that the words contained in the Antisec press release are, in fact, evidence of entrapment. That is, the FBI was encouraging hackers and Anonymous supporters to "fire on," or attack, "any government or agency."

No, folks. Trust your government to do the right thing.