

# THE HACKER NEWS

```
//Find first service  
//Open file found  
ad/write  
me in dta  
puts filehandle into bx  
//Infection  
- offset startvx  
virus lenth/bytes  
vir start [reproduce]  
//Close file  
//Exit  
//All db's  
com",0  
ral/.0x08sn/basic-V1# shutdown 1 "6fc422233a40a75a1f028e11c3cd1140"  
astral@Astral-FX  
21:15 ...  
aintenance in 1 minute!
```

May 2012 , Issue 11

# HACKTIVISM

# *Editorial*

Welcome cyber space readers and internet junkies from around the world. May brings us into an in-depth look at our favorite topic: Hacktivism

Our fearless leader, Mohit Kumar, founder of The Hacker News opens the discussion with a look at the meaning of Hacktivism and what it means for society today.

Our regular writers, security specialist Pierluigi Paganini, and Mourad Ben Lakhousa bring us their perspective on this most interesting and thought provoking topic.

As editor, I truly enjoyed Keith H. DeBus's article on cyber war. I found myself wrapped up in excitement and worry as he takes us into the what's and where's of cyber war.

Also, Dominique C Brack does an excellent job discussing the topic.

Your executive editor, Patti Galle, brings you to question just what anonymous needs to look like in the future and don't miss our fun pokes at current news.

Thanks for your faithful readership and thanks to those who contribute in so many, many ways!

**Mohit Kumar,  
Editor-in-chief,  
The Hacker News**

# Table of Contents

1.) The Awakening of Hacktivism  
Mohit Kumar (Editor-in-chief, THN)

2.) They are Not What You Think They are ...They are Hacktivists  
Pierluigi Paganini

3.) Cyber War: The Asymmetric Paradox  
Keith DeBus

4.) WHO IS WADSON CARLOS?  
Patti Galle (Executive Editor THN)

5.) The Many Faces of Modern Day Hackers  
Dominique C. Brack

6.) Hacktivism : Internet underground for Political Change  
Mourad Ben Lakhoua

7.) Hacking News of the Month  
THN Editorial Staff

Author : Mohit Kumar (Editor-in-chief, THN)

# The Awakening of Hacktivism



Hacktivism (is a combination of two (or more) words or morphemes into one new word (a portmanteau of hack and activism) Hacktivism is the use of computers and computer networks as a means of protest to promote political ends. The term was first coined in 1996 by a member of the Cult of the Dead Cow hacker collective named Omega. If hacking as "illegally breaking into computers" is assumed, then hacktivism could be defined as "the nonviolent use of legal and/or illegal digital tools in pursuit of political ends" ~ Wikipedia, The Free Encyclopedia

Several decades after the most extensive antiwar movement in American history, the protests of the 1960s and 1970s over opposition to American involvement in the Vietnam War, the politically astute of today continue to search for creative ways to “rage on” against social injustices. The most significant lesson that we today can learn from the social movements of the 60s and 70’s is that things could be changed if enough people realize it has to happen. Just like today, the 60’s and 70’s marked a dramatic shift in thinking; as a dramatic rift occurred in the cultural consensus, and a series of subcultures

emerged which could accommodate between them a far wider range of behavior than the 50's style version of conformist consumerism. The same forces fought against in the 60's and 70 are still standing to repress change to this day. These forces seek to pervert the technology and legal systems of our times towards their ends, and the more we tolerate invasions into our freedom and privacy the more of it they will take away from us. The struggle never ends and the outcome must never be taken for granted. Many young people of the 60's and 70's placed their very life on the line for the greater good. Many were beaten, went to jail and some even lost their lives. These modern day activists calling themselves, "Hacktivists" must be brave and bold enough and willing to do the same as their 60's and 70's counter parts. Unlike the 60's and 70's we currently live in an era where political activists have the biggest platform ever developed by mankind: The Internet. At the present time, hacktivists from all corners of the globe have joined together to digitally protest society's ills by way of calculated attacks both serious and at times flippant. Needless to say, the Hacktivists activities of the recent past and in the present have brought with their activism a challenge for transparency to the front line of the global political dialogue and a 21st-century responsibility to safeguard the independence and openness of the Internet from any all forms of assault or censorship.

Just a few short years ago the word "Hacker" would invoke in most peoples minds a vision of geeky teenagers sitting in darkened bedrooms who stole identities and credit cards, and who brandished skillfully their technical knowledge to disseminate mayhem and chaos. However, in the computer world, a hack is merely a quick, intelligent solution to a technical problem. Those individuals that identify themselves as "hackers" may choose to use their knowledge to cripple web sites or protect them i.e. "White-Hats or Black Hats. The world has seen in recent years and months the abilities of individuals and collective groups to use their hacking skills against authoritarian regimes and greedy and unprincipled corporations. It is evident that many "social justice" motivated hackers feel strongly that all conflict emerges from social inequality and those few who use this inequality to their advantage to suppress the unwashed masses and to hold on tightly to their power and wealth. Hacktivists all over the world are coming together and they understand that the world is now facing unbridled dependence on oil, overpopulation, and climate change and all thesees crucial sign posts are signaling the end of secure first-world capitalism as we have known it.

The hand writing is on the wall for all to see that the established social order is facing a radical, impending massive and long needed change. Hacktivists have continued to learn “their” systems, control and manipulated “their” systems, and have and continue to be willing to even shut “their” systems down when they feel there is a need. So what exactly is a hacktivist? Basically, anything a conventional protester, most notably like those of the 60’s and 70’s can do, from graffiti, to general civil disobedience, to sit-ins, can be done online by Hacktivists. So “Rage Against the Machine” continues in a new and unimaginable manner.

Many politically discerning hacktivists of today have become aware that society is an extension of themselves and that the system is made up of hard working, ordinary people like you and me, of men and women with families and children with hopes and dreams. They understand that the balance of power has dramatically shifted away from the majority of people and into the hands of a greedy few. At the moment, all over the globe, political activists understand that the ultimate results of this dramatic shift of power will most certainly be enormous turmoil and violence if the unbalanced and unfair economic conditions continue to deteriorate and are not corrected. They also understand, without a doubt, that political parties both the left and most egregiously the right is failing to provide any reasoned solutions to the escalating social problems and inequalities world wide. While the economic crisis worsens, the foremost responsibility of governments should be to have a strong value system and to redesign their political and economic systems so that there is a fair and proper administration of laws conforming to the natural law that all persons, irrespective of ethnic origin, gender, possessions, race, religion, etc., are to be treated equally and without prejudice.

It is crystal clear that this will never happen without an unparalleled uprising of public support and a full court press of fearless political activism on every possible front. This important present day impetus for global change can be lead by Hacktivists if they take their challenge seriously, live with courage and know exactly who their enemy is and know their enemy well.

# **They are Not What You Think**

## **They are ... They are Hacktivists**

Author : Pierluigi Paganini

During the last couple of years we have witnessed the escalation of operations conducted by the Anonymous group, a hacker group that is expressing social dissent through cyber attacks.

In today's society technology plays a crucial role and is used as a new cultural vehicle, and even an aggregation element or carrier to express dissent against the policies of governments and private companies.

Groups like Anonymous are a maximum expression of a phenomenon defined as "Hacktivism" that refers the usage of computers and computer networks to express social protest or to promote political ideology. If you believe that this form of protest is recent you are wrong, the term, in fact, was introduced for the first time in 1996 by a member of a famous group of hackers the Cult of the Dead Cow hacker named Omega. The hacktivists would attack systems and architectures using legal and illegal tools to perform their operation of protest such as denial-of-service attacks, information theft, data breach, web site defacement, typosquatting and any other methods of digital sabotage. Forms of hacktivism are carried out in the belief that proper use of the technical tools will be able to produce similar results to those produced by regular activism or civil disobedience to promote political ideology.

The Anonymous collective is now the incarnation of the hacktivism concept that has monopolized the world wide attention on the phenomenon. The group and its operations are glaring at the center of this heated debate and public opinion and industry experts are divided between those who believe the collective is a group of cyber criminals and those who take due account of the phenomenon, trying to understand the dynamics of its genesis and not neglecting the value added to their participation in social dialogue.

We must consider that the Internet world is profoundly changing due the continuous acts of hacktivism and the related operations represents one of the major cyber threats. Because the attacks of these groups produced the same effects of those perpetrated by cyber criminals or governments to offend strategic objectives, for these reasons cyber protests must be taken into serious consideration in cyber strategies for the defense of a nation.

According the study “Data Breach Investigations Report” ([http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2012\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)), published by Verizon, hacktivists stole almost twice as many records of ordinary cybercrime from organizations and government agencies.

The most significant change we saw in 2011 was the rise of “hacktivism” against larger organizations worldwide. An impressive number of attacks made by activist with regular frequency have been registered during last year causing a great deal of effort responding to the cyber threat. Cyber activists use hacking techniques to perform their operations involving critical masses made of ordinary people. The type of attack more diffused is without doubts the Distributed Denial of Service (DDoS) attack (<http://securityaffairs.co/wordpress/4468/cyber-crime/ddos-detailed-analysis-of-the-phenomenon.html>), which attempts to make a site or service unavailable to its users due an enormous quantity of requests sent in a short period of time. Hacktivists are demonstrating increasing skills in their attacks and we expect increasing numbers of their operations with possible extensive damage.

In the past, Anonymous supporters have used a program called LOIC allowing them to join in an attack on a particular website, flooding it with unwanted traffic and the group has also released on the web instructions and videos on how to conduct this king of operations. In terms of media, the Anonymous group can be a lesson to many. However, the latest attack I believe represents an element of further development for the group, although it is always a DDoS type, the method used has profoundly changed in the conception.

The recruitment campaign for the attack has also served major social media being able to engage in this way with an impressive number of participants with devastating consequences for victims. Hence the web and social networks like Facebook and Twitter have been flooded by messages of affiliates to the group, a media campaign in style. Anonymous in this way has raised the bar, even a user without his knowledge by simply visiting a web page without interaction, has started to flood a victim with unwanted traffic. The trick is possible simply by hiding within the web pages procedures JavaScript developed specifically that the web browser interprets, then a unique defense option will disable the JavaScript in the browser.

Hacktivism has made a quantum leap with this new method for two simple reasons:

- The first is that without a doubt the offensive force has increased dramatically.
- The second, more subtle but formidable in my opinion, is that from a legal standpoint it is hardly attributable to each user as a criminal liability. A user who participates in the attack, unlike what happened before with Loic, today could not always claim to be aware. This subtle aspect could be stimulus for a wide category of the undecided who share the ideology but fear the incurring legal process by participating in operations.

The cyber war between governments and groups of hacktivists such as Anonymous has an important social connotation as popular movements through technology make known their disagreements and fight for the conquest of freedom. The fight for freedom of expression, the total aversion to any form of control and monitoring, reporting of abuse of power and blatant violations are the main arguments that incite the action groups of hacktivists, however, the boundary between interpretation and of an operation as a simple act of protest or as cybercrime is thin. While many operations are limited to DDoS against a few web sites on more than one occasion, the disclosure of information acquired through hacking systems have exposed sensitive data to public opinions with serious consequences. It happened last Christmas when WikiLeaks published, with the support of Anonymous, more than five million emails <http://pastebin.com/D7sR4zhT> from a Texas-based global security think tank company Stratfor, a global intelligence firm.

WikiLeaks and Anonymous, formed a strategic partnership between the major expression of hacktivism culture, two forces that together are able to frighten the world's great and establish the new alliance against dirty affairs. The hack of the Stratfor Global Intelligence service was made by the same collective Anonymous who disclosed the company website and also the full client list of over 4000 individuals and corporations. They gained access to a subscriber list stored on stratfor.com, and that list contained unencrypted credit card data of the customers. The published emails demonstrated that Stratfor company was providing confidential intelligence services to several corporations, such as Lockheed Martin, and also to government agencies such as the US Department of Homeland Security, the US Marines and the US Defense Intelligence Agency.

The exposed material shows how Government and diplomatic sources all around the world give the Stratfor firm advanced knowledge of the event and of the politic strategies, all in exchange for money. A great spider of informants, government employees, embassy staff and journalists, recruited in everywhere and who are paid through Swiss banks accounts and pre-paid credit cards. The mutual cooperation had already been manifested when the Anonymous group opposed to the actions tied with the founder of WikiLeaks Assange accused of publishing hundreds of thousands of secret U.S. government cables beginning in December 2010. The US government applied as a penalty the block of economic support to the group and PayPal, MasterCard and Visa blocked payments to WikiLeaks, which relied on donations to lease infrastructures. To protest against the penalty, Anonymous arranged massive attacks against these financial institutions. Of course, the actions of groups of hacktivists represent a serious threat to private industry and the national security of each country. The group's attacks have been shown to bring the blocking of services provided by a company, to gain access to sensitive information whose disclosure could undermine the internal balance of a country and its relationship with allied States. And it's for this reason that hacktivism is considered within a cyber strategy a major cyber threat that can cripple with his attacks critical infrastructures, financial services and government agencies.

Groups of hacktivist are considered as uncontrollable variables in the cyber space capable of surprising us with striking operations worthy of the most skilled cyber army.

### **Are we able to mitigate the risks of exposure?**

The cornerstone of the hacktivism is the recruitment of common people through social media to engage in protests, a powerful machine that moves announcing its arrival and producing a loud noise. This undoubtedly provides two advantages:

1. Knowledge of group policies.
2. Ability to operate covert actions against strategic objectives by exploiting the group's operations as a diversionary action.

Governments and law enforcement agencies understand the offensive potential of the group and has accelerated the implementation of measures to control the main channels of communication adopted by hacktivist.

Monitoring systems, increasingly powerful, have been implemented and are being acquired, they are tools able to correlate events and activities within main social media and search engines.

## **Is it possible to use the Group and its function as a cyber weapon? How is it possible?**

It is widely believed that it should carry out intelligence operations aimed at infiltrating the systems and to become an integral part affecting its operations. Similar operations could benefit the needs of groups to involve a critical mass of people for their attacks, unthinkable not to leave traces. In a hypothetical phase the two do not make sense to destroy it. It could be a more profitable influence that their actions against strategic objectives for cyber operations or military operations are behind coverage of diversionary actions conducted by groups like Anonymous. Many consider this approach impractical but it is extremely efficient as cyber weapon using the model of social protest through new media. At this point there may be fake cells of hacktivists recruiting ordinary people directing attacks against institutions and hostile governments. The group has always been driven by purely political motives, and for this reason, imagining it for strategic planning of operations could destabilize an opponent government, exaggerating the tone of the internal political debate. We found that on more than one occasion how dangerous a breath of wind of protest can be through the new social media.

Assuming the possibility of using groups like Anonymous, or rather its model of protest, as a cyber weapon who might be interested in its “recruitment” and what are related risks? Obviously the idea is very appealing to all governments that tend to conceive cyber as aggressive strategies, but that needs to guarantee a low media exposure. How to approach the dangerous groups and with what risks?

Intelligence operations and study of the phenomenon are preparatory to the approach, but with regard to the possibility of infiltrating the group, of course, this could be achieved by conditioning, for example, through financial compensation and other benefits, the medium and high level representatives of the groups, those people that define the strategies of protest. The risks are related to the negotiation with unstable and mutable organizations that we know too little of, but history teaches that such agreements are possible and have occurred in the past such as between states and criminal organizations.

The threat of cybercrime and those made by the actions of protest of groups of hacktivists are sources of considerable concern. Gen. Keith Alexander, current director of the National Security Agency warned regarding the possibility that groups of hacktivist will have the ability in the short term to bring cyber attacks to the national power supplies causing a limited power outage in the US..

Power supplies are just one possible target together with telecommunications systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The profile of cyber assaults against US government and corporate targets is increasing manifesting high skill in the cyber strategy of the attacks. Gen. Alexander declared :

*If forces like those of hacktivist have the technical capacities and critical mass such that they can influencing foreign policy, are we sure that among their goals there are critical infrastructures?*

### **Why we intend to define the components of Anonymous cyber-terrorists and cyber criminals?**

Mr. Richard Stiennon, Chief Research Analyst at IT-HARVEST, draws some distinctions in the definitions as well. A cybercriminal is generally motivated purely by profit. That is a different goal than cyber espionage, which seeks to access intellectual property for military or industrial strategic advantage, or cyberwar, which focuses on actually sabotaging infrastructure, disrupting critical systems, or inflicting physical damage on an enemy.

### **Do you recognize anonymous in one of these definitions? Does Anonymous want this?**

In an official message to the Wall Street Journal Anonymous stated the following regarding the accusation:

*“Ridiculous! Why should Anonymous shut off power grid? Makes no sense! They just want to make you feel afraid.”*

In the past weeks I had anticipated the possibility that someone could use the name Anonymous in other operations, from cybercrime to intelligence operations made by hostile governments, that is why I defined Anonymous a cyber weapon.

The reputation of the group may paradoxically create many problems to the group itself, the audience to which the collective targets is not, in fact, capable of distinguishing false messages, and infiltration attempts that are occurring and will occur with increasing frequency. A mud machine could be set up to discredit the group, or the operation made by unscrupulous criminals who try to benefit from favorable situations for criminal activities, such as to spread malware are useful for realization of fraud. The third hypothesis is anything but fiction that one foreign government is exploiting the emotional involvement in the collective to collect an impressive amount of information on participants in operations.

## **Is hacktivism only a threat or also a voice to listen?**

Some forms of protest are for sure illegal but we must consider that they are expression of dissent shared between large communities. The demonstration is inside the number behind each attacks, these guys are not alone, they have a lot of common people behind them. The main events of protest in history were always characterized by elements of illegality due their connotation of opposing the governments in question. From a legislative perspective we must distinguish hacktivists from cyber criminals. Although the damage of the shares are to be considered in high regard, there are countless methods of judgment about the actions of Anonymous and similar. We must consider the reasons of genesis for these types of movements, otherwise we will not have framed what I consider a historical phenomenon.

In terms of security, the group is without doubt to be considered as a threat due the capabilities shown and objectives selected, politically I think that Anonymous is a voice to be taken into account. Ideologies do not repress it with the arrests.

## **What we can we expect for the future?**

The attacks observed should lead us to some reflections. I think the group is in a time of transition, despite having reached a critical mass of supporters it has begun to split into numerous cells scattered throughout the world. For now, these cells appear to be driven by common goals, but what will happen tomorrow? In a heterogeneous scenario the risk that external agents can infiltrate the group influencing policy is concrete. New operations can be organized with the name of the group with unpredictable consequences, foreign states or law enforcement may involve masses of people and convince unaware hacktivist to conduct ideological battles.

What guarantees can the group provide to its supporters? Will the core of the group like Anonymous be able to capillary check any communication made globally with its brand? Of course not!

I think for this reason that the groups of hacktivists should change their strategies, they are obliged to appear in new forms, probably in the future present itself to the world with their representatives. The time of hiding, in the form of protest could begin to decline. The groups are aware that their attacks may begin to serve to a third cause, not only their own. Analyzing for example the Anonymous case, we must distinguish two phases of Anonymous phenomenon, the first one that I define "Here I am, know me and learn to live with my judgment" is the one we are leaving.

In this phrase the group introduced themselves to the world, showing their offensive capabilities but also established a broad support enjoyed by. The second phase, named "Openness", is the one we will live in the next months. In this phase the group will try to talk with institutions and will operate on the internet but also in the street. This stage is very delicate because of the heterogeneous nature of the groups, many hacktivists will not accept the openness to institutions becoming active in a loose cannon state on the web that could stage striking and unethical attacks.

The worst scenario is that the web may soon reign in the chaos and regulations such as the one under discussion certainly would not be governable.

### **About the Author :**

Pierluigi Paganini, Security Specialist  
CEH - Certified Ethical Hacker, EC Council  
Security Affairs ( <http://securityaffairs.co/wordpress> )  
Email : pierluigi.paganini@securityaffairs.co

## Introduction

In just a brief fifteen years, our communication, commercial and social lives have been dramatically altered by the development and growth of the Internet. With the convenience and bounty of this medium, has also come a dark side. Just as the famous bank robber, Willy Sutton, once said when asked why he robbed banks, "That's where the money is", crime has migrated to the Internet following the money. As e-commerce has grown, so has e-crime. In a few short years, cyber crime has become a leading crime category in the wired



world, costing the global economy \$338 billion in 2011. This is approximately equivalent to the entire GDP of Austria, the world's 27th largest economy. Now, a new, darker frontier in the history of the Internet is being breached and its impact is likely to be even larger than cyber crime on the global economy and global geo-politics, cyber warfare. This short article will attempt to define and elaborate on what cyber war is and the key issues all nations and States must address before responding and retaliating to a cyber war attack.

## Historical Perspective

Since the beginning of human civilization (and probably even few millennia before that), human beings have used physical force to obtain power and treasure. That ancient technique,--physical force-- is what our military strategists now refer to as "kinetic attacks" (cute sanitized term, isn't it?). From time immemorial, armies, navies and air forces launched physical attacks upon opposing armed forces, killing and maiming many and destroying each other's homes, cities and infrastructure. In fact, destroying the others infrastructure has nearly always been a key war strategy. If one nation state can knock out the opponents factories, roads, pipelines, shipping lanes, etc. their ability to sustain a conflict becomes very limited.

Now that our nations and civilizations have evolved and have become more technologically advanced, such kinetic wars may soon be a thing of the past. Imagine, if you will, that instead of bullets, missiles and tanks sent flying from one nation state to another as a form of aggression, that instead, the nation sent cyber attacks to take down critical infrastructure such as communications systems, the power grid, petro-chemical plants, nuclear power plants, and water and sewer systems. Imagine further that the target nation is now without effective communication, electricity and potable water. A cloud of poisonous gases is hovering over major cities from the failure or explosion of their petro-chemical plants and their nuclear power plants are beginning to overheat and their reactor cores meltdown for lack of power to run their cooling pumps. Which would be quicker and more effective at bringing a nation to its knees? This type of surgical cyber attack, or a long drawn out "kinetic attack" that make take years, thousands of lives and trillions of dollars?

## Cyber Warfare Paradox

Curiously, the answer to the above question may depend upon the technical sophistication of the target country. The stronger and more advanced the target country is technologically--meaning it has developed sophisticated communication and infrastructure systems that are dependent upon advanced computer systems-- the more vulnerable they are to an effective cyber attack. This highlights one of the paradoxes of cyber warfare, "***the stronger you are, the more vulnerable you are***". I have coined this, "***The Cyber War Asymmetric Paradox***". Cyber warfare may be the great "leveler" of relative power among nation states as well as between established political and military power and those insurgencies/rebellions/revolts opposed to them. This would also include hacktivists whose efforts to bring attention to their cause would be enhanced by the sophistication/vulnerability of the systems that they are attacking. Among the many wide-ranging impacts the Internet and computer technology have delivered, this leveling of power eventually will be the most significant change we have experienced yet.

This principle of Cyber War Asymmetric Paradox simply states--that unlike kinetic military power-- cyber attacks can be just as effective from a lone--albeit sophisticated --hacker with a \$500 computer (and a bad attitude) as a multi-billion computer system and defense mechanisms. To illustrate my point, imagine a cyber war between the U.S. and Afghanistan. Cyber attackers from Afghanistan could conceivably take out the U.S. electrical grid and other digitally controlled infrastructure rendering the U.S. almost powerless, at least temporarily.

On the other hand, Afghanistan without sophisticated infrastructure would be almost impervious to similar cyber attacks from the U.S. To further expand upon my point, just recently the U.S. space agency, NASA, admitted that they had been hacked into at least 10 times in 2011, despite the fact that they had spent \$58 million dollars per year in computer security (that's not the cost of the computer systems, just the security). With some confidence, I can say that the hackers responsible for these attacks did not spend 1/1,000 (\$58,000) of that amount to carry out these attacks. This illustrates the principle that the cyber battlefield enables an asymmetry of wealth and sophistication of opponents to meet on even ground and, in many cases, the under-funded cyber warrior may actually have an advantage over the heavily funded and more vulnerable opponent. The dependence upon sophisticated computer controlled systems may make the more advanced nation more vulnerable.

## Cyber Warfare Has Arrived

Cyber Warfare is not a tactic of the future--something for us to speculate philosophically about--but rather, it has already begun. At least two events (and probably many more) in recent years seem to indicate that we have embarked upon this novel mode of warfare. The first milestone event was the attack by the Russian Federation on the former Soviet republic of Georgia in August 2008. In this case, Russia and Georgia were disputing the territory of South Ossetia within the borders of Georgia. On August 21, Russians entered the sovereign territory of Georgia to "protect" the citizens of South Ossetia, many of whom are ethnic Russians. For our purposes here, the most interesting part of this attack was that a massive Distributed Denial of Service (DDoS) attack was launched from within the Russian Federation aimed at the computer systems of the Georgian government, effectively shutting down their communication systems and infrastructure during this attack. This DDoS attack played a critical role in the success of that attack.

A second milestone in cyber warfare was crossed in 2010. In that year, a worm appeared in the wild that came to be known as Stuxnet. This very sophisticated worm eventually found its way into the uranium enrichment facility in Iran and effectively disabled the facility by re-coding the programmable logic controllers (PLC) on the centrifuges that control their speed. We need not go into the details of this worm or its impact on Iran's nuclear ambitions here as they can be found in many other sources and have been discussed ad nauseum in the technical and even, general media.

What's critical to us, is that this worm was very specifically designed and targeted to the German-manufactured Siemens digital controllers of this centrifuge . Furthermore, the plant, the centrifuge and the controllers were not connected to the Internet, seemingly making it impervious to Internet-spawned attacks and yet, this worm found its way to its intended and singular target. This marks a new threshold in the sophistication of cyber attacks and may be remembered as the first act of cyber war. The developers of this worm, likely a nation state that both; felt threatened by the Iranian nuclear program and; has the sophisticated programmers to develop such a piece of code (how many nations would that include?). This nation or nations essentially committed an act of cyber war against Iran and did it anonymously and deniably. No one had to launch a missile, a sortie or fire a shot that might leave a trail of attribution. Instead, they simply released a piece of malware into the wild specifically designed for those programmable logic controllers. This piece of software marks a critical watershed in a nation's ability to effectively cyber attack another nation to gain or maintain some political advantage and do it anonymously. Many military cyber war strategists now point to these two events as the first acts of cyber warfare in our NEW world of Warcraft.

## Cyber War Doctrine and Definition

From many reliable sources within the Defense intelligence community, it is reported that the U.S. is the target of thousands of cyber attacks per day. I'm quite certain that the U.S. is not an exception in this regard and that nations across the planet are subject to similar attacks. These attacks range from industrial espionage to attempts to steal state secrets from the U.S. State Department and Department of Defense. Most of these cyber attacks reportedly originate within the Republic of China. These attacks are so persistent, that the military now has a term for them, Advanced Persistent Threats or APT. It is these Advanced Persistent Threats that reportedly were the spur that prompted President Obama to issue his cyber war doctrine. In that doctrine, he has stated that a cyber attack may be considered an act of war and that U.S. may choose to react to such acts as they would any act of war. In the words of one anonymous Pentagon official, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."

Considering the fact that the U.S. has declared that cyber attacks will now be considered an act of war and may be acted upon with an active "kinetic" response, the definition of cyber war may become the most critical definition of our generation.

Every day, literally millions of cyber attacks take place, most by criminal organizations and some probably at the behest of nation states. Some are referred to as Advanced Persistent Threats (APT) by the U.S. military and seem to originate in the Russian Federation and China. Most seem to be in the category of espionage or cyber crime, but where do they cross the line into cyber war?

A simple definition of cyber war might be "When a nation state purposefully cyber attacks another nation's computer systems or digital infrastructure with the intent of political gain or retribution". Sweet and simple, yes? Unfortunately, three (3) key problems exist with this definition for it to have practical applicability.

First, there is the problem of attribution. How can we be certain where or who is behind a cyber attack? The inability of governments, military intelligence or even cybersecurity experts to pinpoint the origin of cyberattacks is problematic. As cybersecurity professionals, we all know that it is possible to trace an IP address to a country, a city or even to a neighborhood. The problem is that IP addresses can be spoofed, attacks can be bounced and pivoted off proxies and the development of "darknet" and such technologies as TOR (actually developed by the U.S. Navy), make it more and more difficult to trace the origins of an attack. Can you imagine the turmoil that a criminal hacker might cause by attacking one nation's key infrastructures and making it look like it a different nation's cyber attack? If the victim nation retaliates with an active kinetic attack, the malevolent hacker/hacktivist might have accomplished the ultimate hack!

This difficulty is not likely to be diminished any time soon as new cloaking, pivoting and proxy technologies advance in parallel to tracking technology. Witness how hard it has been for the U.S. Federal Bureau of Investigation (FBI) to find the members of LulzSec after their forays into hacking U.S. government web sites. Eventually, some were arrested, but only after one member "snitched" on the others. Pretty low-tech attribution.

The second problem with this definition is attempting to determine when an attack is at the instigation of a nation state and not just a criminal organization or hacktivists. The Russian Federation, and reportedly, China as well, have cultivated young hackers with seemingly no state connection and use them for cyber attacks for state purposes.

As stated before, a good example was the Russian Federation's cyber attack on Georgia in August 2008. At the time, Georgia, the former Soviet republic and Russia were in a dispute over the territory of South Ossetia in Georgia. On the day of the attack, a coordinated Distributed Denial of Service (DDoS) attack was launched against the web sites of the Georgian government, effectively disabling them. This attack originated within the Russian Federation, but not from Russian government sources. Instead, several groups of hackers, seemingly independent of the Russian government, instigated this attack giving the Russian government effective deniability.

Further investigation into these groups reveals that they have a long-standing, arms-length relationship with the Russian Federation intelligence and defense institutions. It appears that the Russian Federation has cultivated and probably funded these groups for years, just for such a purpose. Furthermore, because the Russian government owns nearly all the Internet backbone in that country, nothing can happen on the Internet within Russia without the acquiescence and foreknowledge of the Russian government. As this example illustrates, attributing a cyber attack to a particular nation state may be more than a trivial exercise, particularly in the face and heat of a new and ongoing cyber attack.

The third problem with this definition has to do with intent. My definition reads, "Where one nation cyber attacks another nation's computer systems or digital infrastructure with the intention of political gain or retribution". Wars have traditionally been waged between nations that officially declare themselves in conflict. In the world of kinetic war, usually before a physical attack takes place, both nations voice their "displeasure" with the other. When one attacks, we at least have some ostensible intent for the attack. In the world of cyber war, where attribution is extraordinarily difficult, nations may want to keep their intent quiet to hide their attribution.

Cyber war, therefore, may be more like covert operations that the U.S. and the former Soviet Union practiced during the Cold War (and probably are still using) where they used spies and agents to wreak havoc upon each other and their proxies, all the while maintaining deniability. Intention is very difficult to decipher, if the actors are unwilling to voice their intentions. Although it may be relatively easy to define cyber warfare on paper, such a definition leaves much to be desired in practical application.

## Cyber War by Botnet?

Over the last decade or so, those of us in the Information Security field have seen a proliferation of botnets. These botnets allow a master controller to command and control many seemingly innocent and innocuous computer systems for usually some illicit or illegal purposes. Often they are used for such things as DDOS attacks or spamming. In the criminal cyber underground, such botnets can be purchased or leased for any illicit purpose, if you have enough money. Some, such as the Conficker worm that spread around the world in 2008, has yet to be used and no one is quite certain what it is intended for. This could be significant, as some experts have estimated that as many as 25% of the world's PC's are part of one botnet or another.

This problem remains despite the best efforts of Microsoft to patch its Windows vulnerabilities because a significant number of Windows-based operating systems are pirated. Such pirated operating systems are common in developing economies (less so in developed countries, but certainly not unheard of) across the world and very easy to obtain from multiple sources. These pirated operating systems are NOT eligible for Microsoft's security patches and thereby remain vulnerable to new and old rootkits, bots and other malware that solutions have already been developed. This leaves millions of machines available for such bot activities.

One of the potential purposes that I would like to propose here is that these botnets may be preparations for cyber war. They may be groundwork and infrastructure necessary to wage a future cyber war. Imagine, if you will, a nation state that is preparing for cyber war. DDoS and other as yet developed or imagined attacks might require 100,000 or even millions of systems to be effective against a well-protected and secure web site. What better way to prepare for such an attack than infect millions of systems around the globe, some even within the target nation that lay dormant until the time you need them?

When the time is right, these systems can be activated for whatever malicious purposes the malevolent controller intends, at a moment's notice. These might include a DDoS attack upon critical infrastructure or simply to use to launch an attack from within the victim nation to camouflage the origin of the malefactor. Even if these botnets were not developed for this purpose, a malevolent organization or nation state could purchase or lease such a botnet and direct it for such an attack.

## **Conclusion**

Although it may be difficult to define cyber war, we may be certain that it will be an element of any future international conflict. Barring a simultaneous active kinetic attack, though, it may be difficult to actually differentiate an act of cyber war from a criminal or hactivist cyber attack. Among the key issues will be one of attribution and deniability by the cyber aggressor. Without one side clearly stating their intent and willingness to launch an attack, current technologies are inadequate to actually trace the origin of an attack. This may become one of the most prized technologies in the cyber arms race. Finally, and probably most importantly, Cyber Warfare may be the great leveler in geopolitical relations as the "Cyber War Assymetric Paradox" would seem to make the strong the most vulnerable and empower the weak relative to the powerful.

## **Author Info:**

Keith DeBus, President of IT Securitas  
Contact: [keith@itsecuritas.net](mailto:keith@itsecuritas.net)



Author : Patti Galle (Executive Editor THN)

## WHO IS WADSON CARLOS?

All over the globe young people are waking up. This awaking started around 2008-2010 and grew as we witnessed youth driven revolutionary action in Greece, saw the frustration and discontent among young people in Spain and witnessed as a youth driven “Arab Spring” began in Tunisia and rapidly spread into Egypt. It was amazing to witness how young people in Egypt used social media to call for thousands upon thousands of brave people to fill the streets and protest and demanded regime change.

In America young people watched as Wall Street ran a global casino, bringing the world economy to its knees; resulting in young people have a hard time finding jobs and having to stand by helplessly as their parents or themselves lost their homes. In Washington D.C. they saw how elected officials had let them down as greedy corporations flush with millions are buying elected officials and democracy with thousands of high paid lobbyists and copious amounts of money. The youth in America had this sinking feeling that something was not right and the Occupy Wall Street movement was born.

So who is Wadson Carlos? Wadson Carlos is a young Brazilian, and like millions of other young people around the world, Wadson has the same uneasy feelings about the corporate/fascists direction many world governments are heading. Like so many other young people around the world he understands that he like others around the world can't aspire to the lives their parents had, unless they stand up and fight for a different future. Wadson Carlos wants to push against the system.

Wadson considers himself a hacker, an Anon, an important part of a growing number of hundreds of thousands of people who are ready to use modern cyber warfare to bring about a better life for themselves and others. Wadson Carlos is the epitome of most all of the people who have joined the various Anonymous groups to find a sense of companionship and force in a hopeful revolution of change. Still, Wadson is like most in that he lacks the technical skill to use his computer to do what needs to be done. No doubt he and others want to but there is little available to educate cyber dissidents on their weapon.

One only needs to look at history to see that any army devoid of tactical training and specific tasks will eventually wander off and go back home defeated. Here is where I make a call not to the thousands of willing participants who want change but to the seasoned an experienced Anonymous, LulzSec, Hackers, and techies to organize some sort of "cyber training" that will teach our comrades how to do the job.

We need people to perform more than just DDOS attacks. We need a trained army of cyber warriors who know their keyboard and know their weapon. Seasoned cyber warriors need to recognize the army is there, waiting. Wadson Carlos and hundreds of thousands of others, just like him, like you, are yearning for an opportunity to learn how to best utilize the internet to bring political change.

If the Anon phenomenon is really going to do what no other political action groups has been able to accomplish.....bring down the corruption, greed, corporate controlled governments and oppressive corporations that are exploiting the middle and lower economic citizens, poisoning our food, air and waters, we must organize and educate. I leave this to the brightest and committed cyber Anons on the net to decide how to lead your army.

Wadson Carlos and those he represents are depending on you, looking to you, and most importantly, patiently waiting for you. Make your creed credible and take the next step in this epic and demanded revolution. As always, I bow to your sensibility and pay homage to your legions. After all :

**We Are Anonymous  
We Are Legion  
We Do Not Forgive  
We Do Not Forget  
Expect Us!**

# The Many Faces of Modern Day Hackers



The internet and the opportunities it presents to millions of people across the globe are enormous. Many companies today rely on the web for their businesses' operation and many people carry out transactions online. However, in the shadows of the internet, loom some dangers that are not easily detectable, hackers come like thieves and you only realize you have been compromised after they are gone, your privacy is never guaranteed. Someone may be watching and recording every keystroke you make on your personal computer.

Initially, hacking was merely meant for laughs and grins. People would hack into other people's accounts and laugh at whatever they discovered, especially private information. Competing businesses found a clue and would engage the services of the hackers to either fish out information from their competitor's websites or even bring them down. Celebrities have always been the most vulnerable group with hackers sneaking into their personal email accounts to get any information that they deem fit for the ever hungry ear and roaming eye of the public. People have made lots of money from this practice.

## **Key Elements of Hacking**

1. Politically motivated; Most hacking activities orchestrates today are politically motivated with the hackers pushing for a political agenda.
2. Just For Laughs; Some hackers do it for fun. These form are usually not financially motivated
3. Financial Motivation: Many people have lost lots of cash through the hackers who steal passwords and personal information.
4. Anonymous: Most hackers are unknown even to the public and tracing them is not easy. This is because it can be carried out remotely over transnational borders
5. Solo Activity: For activism to be successful there is always need for a mass following. On the contrary, hacktivism can be carried out by an individual or a very small group of hackers

## **Hacktivism**

On realization that they are being fought from all corners; by individuals, corporate, and governments, the hackers saw the need of coming together. Today, they are several organized groups that champion different causes. One of the most common reasons for organized hacking of prominent people's accounts has been to protest bad leadership that is collectively referred to as hacktivism. Just like activism where civil and human rights groups use all means possible to champion their courses, hacktivism involves the use of the internet by hackers to send out serious targeted messages to governments, individuals and groups that try to gag the internet, overall bad leadership and bad policies. Most importantly, they demand the freedom of the cyberspace.

## **The Police Crackdown-Chasing the Shadows**

Governments across the world are always on the lookout for hackers. Employing all the available technological tools available, they have managed to make some successful arrests. In the United States, the FBI has successfully brought to book key members of a hacking group that is only known as "Anonymous."

## **The Anonymous**

When one is attacked or mugged during the day, there is always a possibility of identifying the person. It is a whole different story when you come face to face with a gang of robbers in a dark alley in the middle of the night. The only thing that will be clear will be; you were robbed. Any other details regarding who might have done it will remain elusive for a long time.

That is why the hacking group “anonymous” is always having a field day on the web. There is no doubt that the group is comprised of the sharpest brains and internet gurus. With members spread across the continent, “Anonymous” agitates for the freedom of the internet and is against the internet related legislations.

## **WikiLeaks- The Whistleblower**

Julian Assange is one intelligent fellow who earned global admiration and hatred in equal measure with his damaging leaks-the wikileaks. This is the man whose organization doesn’t target the small fish or struggling corporate. He is global, and he has built a name based on that. The United States is a super power and when Assange exposed the goings on in Uncle Sam’s life, mouths were left agape and governments all over the world held their breath, anxiously waiting.

Since most of the wikileaks were authentic enough, the media was quick to feed the hungry audience with as much information from wikileaks as possible. Before he knew it, the man was roughed up by the police. Citizens from all the corners of the world and the hackers felt they were being cheated as they had the right to know.

Different companies decided to cut ties with wikileaks, including Mastercard, paypal, Swissbank Post Finance among others. They refused to process donations for the whistleblower from many people who obviously believed in their course. However, it wasn’t long before Anonymous hacked and paralyzed the operation of mastercard on Wednesday, Dec 8, 2011.

## **Anonymous Revenges, Hacks Mastercard**

To stand in for their brother, Asange and Wikileaks, the notorious online hacktivist group Anaonymous decided to teach some companies a lesson. When the international credit card company Mastercard decided to cease taking donation to Wikileaks, Anonymous set out to teach it a lesson, plus others.

They orchestrated a DDOS (Distributed Denial of Service) attack on the website halting operation to many users. This was dubbed the “Operation Payback.” After the successful attack on the card company, the group vowed to target Paypal, which had also refused to process payments for Wikileaks.

## **The Operation Hackerazzi**

The most vulnerable group to hackers is the celebrities. In the past, most celebrities have done everything to avoid the flashes of cameras that are planted everywhere by paparazzi. To a journalist, every second in a celebrity's life may result into some captivating news. As a result, they stalk them everywhere they go, hide in dark alleys and can go as far as bribing their domestic staff to plant minute cameras in their bathrooms, bedrooms and any of their perceived personal space to get the exclusive picture, or just hear their conversations. That was before the FBI in Los Angeles hunted down and arrested a celebrity hacker in an operation that dubbed "operation hackerazzi."

To the 35 year old Florida hacker, Christopher Chaney, hacking celebrities is some form of addiction. Having hacked into the emails of celebrities including Christina Aquilera, Mila Kunis, Scarlet Johansson, he must have been enjoying the whole experience, even though he later apologized for the actions. The man was faced with 26 counts of identity theft, wire tapping and unauthorized entry into protected personal computers. With all these accounts, the celebrity hacker stands a chance of spending the next 121 years behind the bars of a cold cellar.

One of the most successful celebrity hackerazzi that was orchestrated by Chaney was the Scarlet Johansson nude photos saga. The celebrity was quick to point out that the pictures were meant for her now divorced husband Ryan Reynolds. The damage had however been caused and her privacy exposed by Chaney. The operation hackerazzi is said to have taken a whole year, just to bring one celebrity hacker to book.

## **Anonymous-Wikileaks Alliance-Union Made in Heaven!**

Hacktivism is taking a fresh dimension, joining forces to advance a common course. In Dec 2011, the hacking group Anonymous hacked Stratfor, a US based security think tank. They later claimed they had over 5 million emails from the company and they were set to expose the rot in Uncle Sam for its crackdown on innocent citizens and hacktivists.

Anonymous is ultimately the best organized hacking group on the web. Recently, on allegation of corruption, Anonymous hacked into the Vatican website as well as the Vatican's newspaper. On the other hand, Wikileaks has perfected the art of sorting out the information and dealing with the media.

## **The Future of Hacktivism**

The governments across the world must be learning a lesson the hard way. Even though the police intelligences all over the world are trying everything to bring the hackers to book, it is not an easy task. There are numerous hackers organization in the world today whose tracking and arrests is not an easy task. The more they are arrested, the more they perfect the hacking. They are now coming together and forming alliances across the World Wide Web and with no chance of relenting in their quest for a freer web and a just society. The public supports and funds the hacktivists as they believe in their courses. At personal levels, everyone must protect himself/herself against hackerazzis and those who are after your money.

## **Top Five Ways to Cushion Yourself against Hackers**

1. Don't divulge personal information to anyone on web
2. Use a unique and strong password, mix alphabets, numbers and symbols
3. Regularly change your passwords online
4. Install a security softwares on your PC
5. Don't click on unknown URLs and open attachments on anonymous or suspicious emails

It may be discouraging watching large government bodies and celebrities' websites being hacked into. However, you can avoid the occurrence of the same by being extra cautious and observing high degree of privacy.

**About the Author :** Dominique C. Brack, CEO Reputelligence™  
CEI - Certified Ethical Hacker Instructor, EC Council

Dominique C. Brack is a recognized expert in information security, including identity theft, social media exposure, data breach, cyber security, human manipulation and online reputation management. He is a highly qualified, top-performing professional with outstanding experience and achievements within key IT security, risk and project management roles confirming expertise in delivering innovative, customer-responsive projects and services in highly sensitive environments on an international scale. Besides his work as management consultant, advisor to the government and CEO of Reputelligence™, he has lectured at trade shows and conferences and is the author of various articles and white papers.

<http://www.reputelligence.com> | Email : dbrack[at]reputelligence.com

# HACKTIVISM

INTERNET UNDERGROUND FOR POLITICAL CHANGE

Author : Mourad Ben Lakhoud

Cyber-attacks are appearing in several forms and purposes. Gaining income is one of the first objectives but as it is getting easier to conduct these attacks we are seeing other objectives like hacktivism using hacking technology for making a political change.

Hacking tools are available for any user without restriction and they allow the attacking of any target including defacing websites to transmit certain political messages mostly by conducting a distributed denial of service to put pressure on targets or dumping and leaking database sensitive information and posting them online to threaten the victim and make them accept others ideas.

Hacktivism is not a new phenomenon. Here are three previous incidents: The first in 1998 hacktivists attacked Mexican President Zedillo's website to make it slow and bring attention to Zapatista rebellion.



INTERNET UNDERGROUND

The second example is the nike.com attack in 2000 where attackers redirected visitors to a global capitalism problem website. The third is a hacktivists DDoS attack on Iranian government websites that are paralleled with street protests due to no transparent elections.

Regardless of the political change wanted that are behind the cyber attacks, most previous incidents showed how much systems and government infrastructure are vulnerable to attacks. LOIC as a DDOS tool have been used for taking down any website to make it unreachable and here it is noted that DDoS is 100% successful.

On the other hand most people that are arrested for these attacks are teenagers which shows that there is a lot of technical awareness for this critical age and the attacks are so simple. DDOS tools (LOIC) are available online. It is easy for someone to be arrested simply because they are not educated enough to understand the process of using these simple methods.

When the strike comes to any government or organization security becomes a dream that may not be true, dreaming is good but the question remains what security measures are in place to protect the infrastructure?



*Iranian election Twitter was used to support virtual riots via DDoS*

mitigate risks of social engineering attacks and classify any action performed by any member.

Achieving security is by covering several steps and stakeholders that include:

## 1. Security Policies

Having clear security policies in place will play a big role in understanding laws, security procedures and can be an important step in organizing relations between stakeholders, so this will

## 2. Human Resources awareness

Conducting a personnel training and awareness programs on security topics will make your employees ready and aware about risks of cyber attacks and can play a big role in mitigating being the next victim.

### **3. Security Skills**

Security skills are important in handling any attack as during a DDoS attack you need a highly technical team that may follow and stop sources of attack with a coordinated network that will keep you alive and connected with the cyberspace.

### **4. Technical Security**

Technology is important to handle such attacks so having in place an Intrusion detection and prevention system, load balancing and resilient architecture solution for availability issues, monitoring solution that will record and provide you a dashboard to control the situation during the attack, this all besides an encryption solution that will keep your data out of hacktivist hands.

#### **Reference:**

# Hacktivism and the Future of Political Participation

<http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf>

# Richard Stiennon presentation defending against a new generation of security threats

[http://www.theitservicessite.com/webinar.asp?webinar\\_id=29820](http://www.theitservicessite.com/webinar.asp?webinar_id=29820)

#### **About Author :**

Mourad Ben Lakhoua is an Information Security practitioner.

Admin at [www.sectechno.com](http://www.sectechno.com) | [info@sectechno.com](mailto:info@sectechno.com)

# News of the Month

# Google's rogue engineer Maps your Quests while you remain lost  
<http://goo.gl/256Zc>

# Hacker claims to hack European Space Agency, NASA, US Air Force and Military, French Ministry of Defence : <http://goo.gl/zjdlg>

# Crime does pay as flashback malware Creater earning \$10,000 per day from Google Ads : <http://goo.gl/Wp2Eh>

# While you're chatting Skype is Exposing User IP Addresses :  
<http://goo.gl/IEYGW>

# Fed up with billy clubs, pepper spray, and abuse, the International Police Association website defaced by Anonymous Hackers :  
<http://goo.gl/uGGnI>

# Afghan Taliban website hacked 3rd time by hackers; Tailban too busy launching matches to care : <http://goo.gl/nDZE8>

# Don't look now but more than 100000 Wireless Routers have Default Backdoor : <http://goo.gl/ltpxo>

# Facebook source code hacker explains,what really happened ! :  
<http://goo.gl/evMSl>

# 0Day Remote Password Reset Vulnerability in MSN Hotmail patched : <http://goo.gl/gAnp5>

# Chinese Hackers ran out of Mango's and continued to attack the Philippine government : <http://goo.gl/oRm8T>

# Iran Preparing For Cyberwar Against U.S. and we are really, really, afraid..... : <http://goo.gl/DEFrM>

# VMWare Source Code leaked by Anonymous Hackers :  
<http://goo.gl/Iod2V>

# News of the Month

- # New Flashback malware variant found in the wild along with salmon and other fish : <http://goo.gl/LHBiL>
- # Cyber Attack on The Iranian Oil Ministry's Computer Network got really greasy : <http://goo.gl/RvrKI>
- # Iran Replicating Captured U.S. Drone RQ-170 Sentinel. Matel will copy their replication : <http://goo.gl/phb71>
- # TapLogger Android Trojan can Determine Tapped Keys : <http://goo.gl/VuWpa>
- # Specialized Trojan can steal credit card details from hotel. More US FBI/CIA agents will be caught doing the deed! : <http://goo.gl/igfVv>
- # Anonymous Hackers target F1 website in Bahrain GP protest : <http://goo.gl/pZnQn>
- # Lebanese Government sites hacked by 'Raise Your Voice'. Apparently, they weren't listening : <http://goo.gl/uoALQ>
- # MI6, CIA and Department of Justice Tango Down ! OH YEAH BABY! : <http://goo.gl/oxGeo>
- # Banking System Vulnerability - 3 million bank accounts hacked in Iran while Iranians were busy thinking they could do a cyber attack on the US : <http://goo.gl/PeDxT>
- # Stuxnet was planted by Iranian double agent using memory stick : <http://goo.gl/OazYN>
- # FBI track Anonymous hacker using his girlfriend's boobs. His dick was busy. : <http://goo.gl/eYLYn>

# News of the Month

# Botnets, DDoS attacks as weapon against financial sector :  
<http://goo.gl/SJoNr>

# Phone based denial-of-service (DoS) attack on MI6 Anti-terrorism Agency. One ring-a-ding, Two ring-a-ding..... :  
<http://goo.gl/xHOo4>

# Homeland Security hacking into gaming consoles to obtain user data : Since they can't hack into major cyber threats they pick on the gamers.....assholes : <http://goo.gl/oaIK8>

# Anonymous target USTelecom and TechAmerica for supporting Cybersecurity Bill. CISPA supporters, be afraid....be very afraid.....you assholes : <http://goo.gl/LLCJR>