Hacktivism

François PAGET (Researcher chez McAfee Labs)

July 2013, Article n°II.3

In the field of computer security, hacktivism covers a substantial part of current cyber-threats. In the following pages, we will go into the details of those who claim to be part of it, and compare their motivations, their modus operandi, and the impacts of their actions to those of other cyber-criminals.

Hacktivism at the center of cybercrime

There are many different types of cybercriminals. Specialists have therefore built their own typology for cybercriminal felons. We will focus on three of them.
The first goes back to 2012, and came from Raoul Chiesa, who created it at the beginning of the second phase of his study on hacktivists' profiles (The Hackers Profiling Project – HPP V2.0 – 2011-2015) [1]. Presented in the chart below, his ranking is still provisional and details 9 distinctive profiles.

Profile	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they may act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

FIGURE 1:Cybercriminal profiles(according to ROBERT CHIESA)

[1] http://www.flemminggulf.com/cms/uploads/conference/downloads/Raoul%20Chiesa%20DAY%202.pdf

In such a ranking, the hacktivist can be put in any of these categories: he can be a script kiddy[2], an ethical hacker or a cyberwarrior.

A second representation is shown in the Verizon report [3] of April 2013. Here, the starting point is the genesis of the attacker from the group organized crime, state or activism).

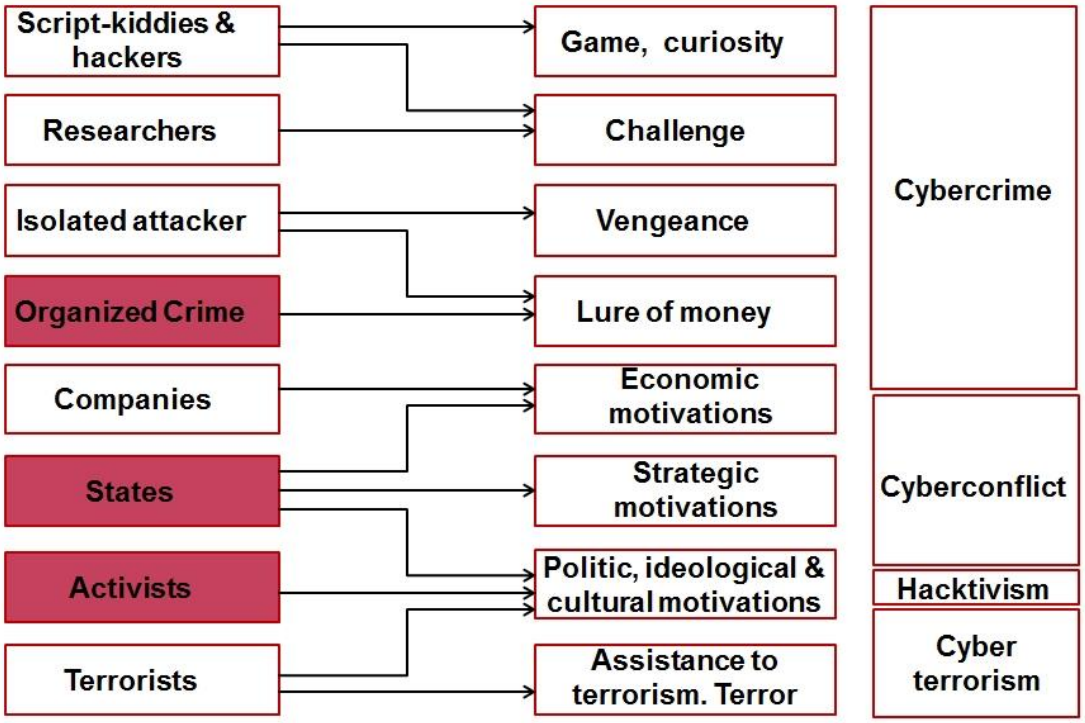
	ORGANIZED CRIME	STATE-AFFILIATED	ACTIVISTS
VICTIM INDUSTRY	Finance Retail Food	Manufacturing Professional Transportation	Information Public Other Services
REGION OF OPERATION	Eastern Europe North America	East Asia (China)	Western Europe North America
COMMON ACTIONS	Tampering (Physical) Brute force (Hacking) Spyware (Malware) Capture stored data (Malware) Adminware (Malware) RAM Scraper (Malware)	Backdoor (Malware) Phishing (Social) Command/Control (C2) (Malware, Hacking) Export data (Malware) Password dumper (Malware) Downloader (Malware) Stolen creds (Hacking)	SQLi (Hacking) Stolen creds (Hacking) Brute force (Hacking) RFI (Hacking) Backdoor (Malware)
TARGETED ASSETS	ATM POS controller POS terminal Database Desktop	Laptop/desktop File server Mail server Directory server	Web application Database Mail server
DESIRED DATA	Payment cards Credentials Bank account info	Credentials Internal organization data Trade secrets System info	Personal info Credentials Internal organization data

2ND FIGURE: CYBERCRIMINAL PROFILES (VERIZON SOURCE)

Unrepresented in this chart, yet considered in this report, one also finds companies, along with their staff and business contacts, and isolated people.

Studies focused on various cybercriminals, including the two exposed above, have led me to create the chart below, in which can be found all of the involved actors (on the left), and, highlighted in red, the three main current profiles : organized crime, states and hacktivists.

[2] They range from 10 to 18 years old. If younger, they are sometimes callsed lamers or packet monkeys
[3] http://www.verizonenterprise.com/DBIR/13/



3rd FIGURE : CYBERCRIMINAL PROFILES (SOURCE : FRANCOIS PAGET - MCAFEE)

At the center of this graph, and linked to the agents, are their main motivations. Obviously, exceptions exist, and that an ill-intentioned agent, under the cover of his company, can act out of vengeance.

To the right, the various levels of confrontation are listed, according to the agents' motivations and the targets they confront themselves to. One sees that the intentions of hacktivists can overlap with cyberconflicts[4] and cyberterrorism.

Hacktivism: A meeting point between hackers and activists.

Hacktivism is a neologism which stems from hacker and activists. It seems to have been used for the first time by a member of the "Cult of the Dead Cow" group[5] (to describe hacking for political purposes[6]).

Definition of the term « hacker »

In the 80s, far less known than today, the term « hacker » was used merely by avid computer experts and bore a rather positive connotation (for instance, Stephen Levy's book

[4] In this graph, the term « cyberconflict » is prefered to the term « cyberwar ». The term « war » implies a simultaneous armed conflict. Even though hacker attacks can jeopardize a state's sovereignty, they do not necessarily occur in the course of an armed conflict, because the level of violence is somewhat lower.

[5] Hacking Organization founded in 1984, in Lubbock, Texas, United States. It is known for having created, among others, Back Orifice, in 1998; a client/server program which enables remote control of Windows-operating devices.

[6] Hacktivism: From Here to There: http://www.cultdeadcow.com/cDc_files/cDc-0384.html

published in 1984, which bears the title : Heroes of the computer revolution.)[7]

In spite of a slightly aggressive side to it, the term expressed an ideal, which manifested in favor of free, decentralized and shared information.
The term's connotation moved over the years, becoming slowly a synonym of computer theft or vandalism. Nowadays, the word carried many different definitions. Positive, pejorative or negative, they range from brilliant and passionate computer programmers, promoters of open source to simple hobbyists, and criminal intruders who gain access to computer systems to steal or delete information.

In a reference to American western movie archetypes, hackers were then classified by reference to the colors of the hats worn by the cowboy heroes (the white belonging to the goodie, the dark hat belonging to the baddie).
The term is still used today, even though the origin is forgotten by many. A third color has been added: grey hats. One therefore finds:

- White hat hackers who don't venture into illegality. He talks about computer intrusion, programming and hacking techniques with others. He often pictures himself as a computer security enthusiast and wants to help his relations. If he discovers a breach, he will not reveal it publicly but disclose it, often with no compensation, to computer specialists who will then close it.
- Grey hat hackers study and test criminal methods. Without destroying anything, they de trespass into computer networks. If he does find a breach, a subversive program, or a way to crack a software program, he will share his discovery with everyone, with no concern as to the consequences of his actions, nor of the legal implications. Faithful only to his own code, he can also sell his skills and discoveries to the highest bidder.
- The black hat hacker breaks the law on a regular basis. He uses his skills in a destructive manner and represents an actual threat. He penetrates computer networks in order to harm the people and companies they belong to.

Not to be conflated with hackers, script-kiddies use programs and techniques, without really understanding them and therefore in a clumsy way. The purpose can range from simple leisure to outright vandalism.

Definition of activism

According to the Larousse dictionary, activism is a code of conduct which promotes direct action[8], in particular on political and social grounds. Law teachers Raymonde Crête and Stéphane Rousseau, on the other hand, quoted a translated definition in 1997, in their books[9], of the Merriam Webster's Collegiate Dictionary (10th edition) and of the American Heritage Dictionary. They defined activism as "a doctrine or practice which favors direct and vigorous actions, particularly to take position for or against a controversial stance" or " a theory or a practice based upon " a militant action".

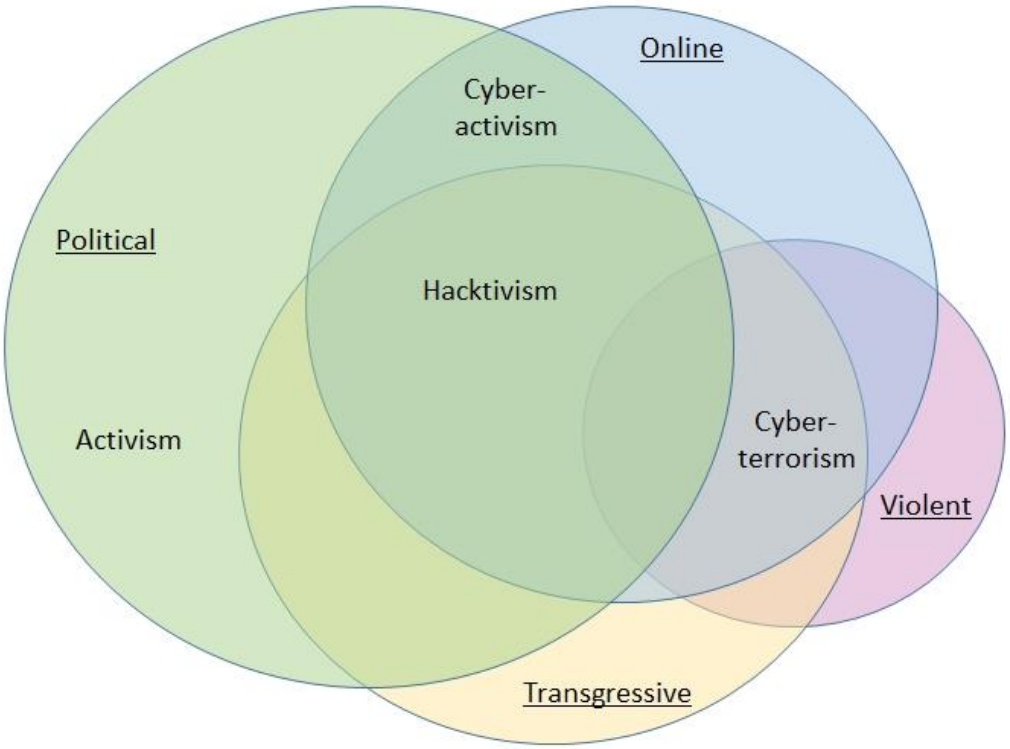
---

7 http://digital.library.upenn.edu/webbin/gutbook/lookup?num=729
8 http://www.larousse.fr/dictionnaires/francais/activisme/945
9 Crête R. et Rousseau S. (1997), « De la passivité à l'activisme des investisseurs institutionnels au sein des corporations : le reflet de la diversité des facteurs d'influence ». http://lawjournal.mcgill.ca/documents/42.CreteRousseau.pdf

Cyber-activism & hacktivism

Sometimes close to libertarian activism (and its desire to preserve freedom to undertake, individual liberties, freedom of speech, data circulation freedom), activists on the Web gradually engaged in the construction of online activism. Like other activists who don't hesitate to trespass onto the forbidden perimeter of European nuclear plants[10], those who promote their ideology but prefer to remain virtual, have decided the grant themselves the right, on the grounds of their belief, to penetrate off-limit digital areas.

For Pr. Dorothy Denning, hacktivism is defined by "operations involving the use of hacking techniques within websites, designed to disrupt the normal activity, but without intent of causing important harm".[11] In a 2012 document, the CEIS company presented[12]:



4th FIGURE : Activists' profiles(SOURCE :CEIS)

Alexandra Samuel's definition[13] is illustrated here, as she defines the movement as « the non-violent use of digital illegal or aggressive equipment, for political purposes ».

This graph and this definition are interesting because they enable a clear distinction between hacktivists and cyber-activists. The latter does not use aggressive means to express himself but simply transposes his "activism" into cyberspace (email, tweets,

10 As was the case for the plants of Bugey and Civaux, on May 2, 2012.
11 http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (page 241)
12 http://www.defense.gouv.fr/content/download/200639/2219639/file/OMC2012T3.pdf
13 Alexandra SAMUEL, Hacktivism and the Future of Political Participation, Thèse de l'Université de Harvard, Cambridge Massachusetts, september 2004, p.2 : "hacktivism is the non violent use of illegal or legally ambiguous digital tools in pursuit of political ends".
http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf

or Facebook status, blogging). He leaves the former to perform more radical actions, thus regularly breaking the law (site disruption, service denial, hacking, etc.)

Hacktivism and cyber-terrorism

Activism, eco-terrorism and terrorism are sometimes conflated. Nowadays, some non-specialized publications even lend such activities to members of Al-Qaeda[14]. This diversity of points of view stresses how difficult defining this term can be, when the specific denotations can vary from one country to another, according to whether it is seen, by our standards, as democratic, authoritarian, religious, or extremist.

By integrating the concept of violence, the graph below (4th graph) enables to differentiate hacktivism and cyber-terrorism.

Even within the Anonymous group, opinions differ. According to Mark Pollitt's definition ("premeditated attack and motivated policy against information systems, software programs and date by sub-national groups or clandestine agents, from which violent actions on non-combating targets[15] are induced"), certain actions from the group can therefore be qualified of cyber-terrorism. However, Dorothy Denning, in 2001, insists on the fact that terrorists, even when they use the Internet, will always prefer bombs to bytes[16], and her definition of "serious damage" is not necessarily the same as what Mark Pollitt calls "acts of violence".

As for us, we do use a scale of violence to define whether a militant act is that of an activist or a hacktivist. For instance, some Yemenites perform activist actions in order to fight in a peaceful fashion against the American policy and the use of drones to eliminate djihad warriors of AQAP (Al Qaeda in the Arabian Peninsula)

The question stands, whether the groups we will further describe, such as the Anonymous, leave or not the hacktivist realm when they gain access to military or diplomatic confidential documents (or even top-secret) and disclose them, as it occurred on several occasions through Wikileaks.

Hacktivist profiles

Under the term hacktivist lie many different profiles. Here are the 4 most notorious.

Anonymous

Most hacktivists unite under the Anonymous banner. Their cooperative activism is based on teams of individuals focused on defending various local causes to global movements such as anti-globalization or anti-scientology. Many "post-it" activists[17] tend to join them, active at some times, dormant at others, but on (connected) standby, ready to act for the group whenever a project they deem worthy to serve arises. Anonymous is therefore more an idea than it is a group. It is a network of networks which comes together and falls apart, to the rhythm of projects and opportunities.

Anonymous was revealed to the public when they supported Wikileaks in 2011. They were portrayed in lenient light by some, when others considered them to be criminals in a new form. A year and a half later, internal tensions and the absence of clearly stated targets made them lose

14 http://www.20minutes.fr/ledirect/1079689/yemen-arrestation-deux-activistes-al-qaida

15 http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

16 http://faculty.nps.edu/dedennin/publications/Cyberwarriors%20-%20Harvard.pdf

17 http://www.cesep.be/ETUDES/ENJEUX/De%20l'activisme%20en%20ligne%20au%20militantisme%20de%20terrain%20_%20les%20nouvelles%20formes%20d'engagement%20Etude%20CESEP%202012.pdf (read page 4)

popular support. Moreover, their absolute demand for anonymity is disgruntling to some NGOs who would like to benefit from the ill-mastered support they gather. Always short-lived but also sometimes very disruptive, the actions of Anonymous remained as numerous in 2013 as they were in 2011.

Pseudo Cyber-armies

Other hacktivists are found in groups who dub themselves "cyber-armies". In its first quarterly report of 2013[18], McAfee listed 14 of them, which had carried out actions in the first quarter of the year.
The list is below:

- 3xp1r3 Cyber Army (Bangladesh),
- Afghan Cyber Army,
- Alarakai Cyber Army (who claim to be close to al-Qaeda),
- Armenian Cyber Army,
- Bangladesh Cyber Army,
- Brazilian Cyber Army,
- Indian Cyber Army,
- Iranian Cyber Army,
- Muslin Liberation Army (MLA),
- Pakistan Cyber Army,
- Philippine Cyber Army,
- Syrian Electronic Army (SEA),
- Tunisian Cyber Army,
- Turkey Cyber Army.

The countries these groups originate from are found, as all the others are, in the Reporters Sans Frontières report, in the world ranking for freedom of the press. Among them, the best placed country is number 1 (Finland), the worst placed is number 179. Armenia excluded, all of the countries harboring these cyber-armies are beyond the ranking of 100. And 9 of the 13 are ranked between 138 and 176.
Claiming that these groups flourish mainly in totalitarian and extremist countries therefore stands to reason.

Their members are patriots (genuine or manipulated), and often qualified of cyber-warriors. They claim to act on behalf of their government and often promote ultra-nationalistic causes. Their real political engagement is often limited and their ideology blunt.
The line between Anonymous and "cyber-armies" is however thin and porous, the former supporting the latter, on-and-off. This happened on several occasions during the Israeli-Palestinian conflict.[19]

These groups perform low-intensity attacks (short-lived DDoS attacks[20], site defacing). When the technical competence is high, it seems reasonable to call them cyber-terrorists (or terrorism-abetting).

---

[18] http://www.mcafee.com/au/resources/reports/rp-quarterly-threat-q1-2013.pdf

[19] Operation Pilar of Defense - Anon declares "war" on the IDF (Official Israel Defense Forces), thus joining the hacktivists Pakistani anti-Israeli groups : http://www.cyberwarnews.info/2012/12/01/300-sites-hacked-by-anonymous-pakistan/

[20] DDoS (Distributed Denial of service) : A computer attack aiming at making unavailable to legitimate users an online service. It can block a file server, cut off a web server, prevent the distribution of email within a company or make a website unavailable.
A Denial of Service (DoS) is caused by a single source. If several devices, spread out on the network, form what is most often a botnet, the attack is named a Distributed Denial of Service.

Militants

More integrated than the Anonymous and opposed to the ideas shared by cyber-warriors on freedom of expression, more thought-out militants can be found, who mainly use the Internet and social media as a means of communication, propaganda and intelligence. Semi-hacktivists and semi-cyber-activists (according to whether they break the law or not), they include sympathizers from the "Indignés" movement and "Occupy", who no longer grant legitimacy to the economic and political powers they are subjected to.

The Telecomix group is the perfect example of this double identity. As cyber-activist, they have supported, from abroad, the Arab revolutions and are close today of the opponents of the Notre-Dame-des-Landes airport. As hacktivists, they participated to the mirroring of the CopWatch site, in 2010, after it was banned from access on French territory[21]. They sometimes mock the Anonymous which they depict as agitated kids with little technical know-how.

In January of 2013, militants from the hacktivist cause, possible precursors to digital anti-globalization activists of tomorrow, initiated a campaign to legalize militant DDoS. Conflating defacing to displaying a banner, and comparing DDoS to a sit-in in front an entity they wish to block, they suggested the creation, similar to what already exists is conventional demonstrations, an upstream declaration process to the authorities. The dates, targets and duration of the digital blockades would therefore be known in advance. Hinting at the birth of ONG 2.0, ideologically debatable but respectable within our democracies, they suggested the creation of an upstream declaration form, much like what already exists for traditional demonstrations: the dates, targets and duration of the digital blockade would therefore be known in advance. Hinting towards the appearance of ONG 2.0, ideologically debatable but respevtable within our democracies, they suggested the creation of declared institutions, established and recognized onto the Web, able to lead protestations in the same fashion a union or a political party would in real life. A petition which gathered a mere few thousand signatures was handed to the White House website.[22]

Opportunists

The hacktivist movement also harbors a great many opportunists who deal in piracy and completely uncontrolled defacing. Claiming to spread a message, they seem in fact only motivated by sportsmanship or quantitative achievement: the winner being the one who hacks in the most flamboyant way or the largest number of sites in a given time.

Conclusion

After supporting Wikileaks, at the end of 2010, the large-scale operations launched by Anonymous the following year (#OpSony, operation GreenRight, #Antisec, #OpCartel) promoted libertarian ideas. They were somewhat successful and followed by a few other large-scal operations in 2012, but those were more limited in time (#OpMegaUpload, operation Stop SOPA, #OpWcit, #OpWestBoroChurch, #OpAngel).

For a year, we have entered a phase where the mere Anonymous signature is often left aside. And even if the slogan "We are Legion. We don't forgive. We don't forget. Fear us." is still as used, those who do quote it make sure they sign their actions with the name of a group or an ideology which they wish to be more recognizable. The simple Guy Fawkes mask doesn't suffice anymore: the game is to remain anonymous while getting noticed, so as to claim responsibility for the attacks. A large number of representing operations from 2013 (#OpIsrael, #OpUSA, #OpPetrol, etc.) are of that order. Using the imagery created by Anonymous, they are the work of individuals operating out of the Middle-East and North Africa, whose jihad-oriented tendencies are freely unveiled in their communications.

---

21 http://fr.scribd.com/doc/68777613/20111014-TGI-Paris-Copwatch

22 http://www.01net.com/editorial/583847/anonymous-une-petition-pour-que-les-attaques-en-ddos-deviennent-legales/

The hacktivist movement is radicalizing. When yesterday's hacktivists worried about our liberties, the rallying cried heard today promote far more extreme ideologies, and far less respectable. The voice of the freedom-loving militant is quashed by the cyber warrior's. This new deal only amplifies the threats which loom above our democracies which should take this new parameter very seriously.