Positions between the law and hacktivist actions

Mrs Cécile DOUTRIAUX is a lawyer, and a graduate from the conservatoire national des Arts et Métiers, civilian reserve officer in the gendarmerie nationale and a member of the cyberdefense and cybersecurity chair in the Saint-Cyr Coëtquidan schools.

October 2013 – Article n°II.4

Cyberspace has become a power challenge, not only for states, but also for social groups, claiming a certain ideal. Thus, the Internet has become a preferred direct action mode for hacktivists, confronted to a political system which hampers protestation and opposition with legal means. Hacktivists, who use new technologies and hacker methods to spread their political claims, are perfectly aware that information systems can provide states with a strategic tool to monitor populations. How do hacktivists relate to the law, facing this attempt to control them? What are the state's means to repress and to maintain law and order, facing hacktivist actions, especially when classified information is released to the public and foreign states?

Hacktivists' relation to the law and position of the law facing hacktivists.

Cyberspace, long seen as a limitless, universal and self-regulated environment, is very coveted, nowadays. Insofar as its borders are uncertain and dictated mainly by its networks, both private and public, commercial and governmental, it has become an important political and ideological territory to infiltrate and conquer. This territory has become a power challenge, not only for states, but also for social groups who promote a certain ideal.

Cyberspace is a ring for ideological confrontation, facilitated by digital tools which allow for global, easy and quick spreading of ideas. Thus, the Internet has become the preferred direct action mode for activists, confronted to a political system which hampers protestation and opposition, through legal means or not, according to how democratic the state is.

To promote their ideas, to make a show of force in terms of communication and command of information systems, some activists will cross the threshold of cyberactivism, which is embodied by the use of social networks to protestation ends, to borrow some of the hackers' methods. Therefore, hacktivism is the use of new information and communication technologies and hacking techniques, by activists, to spread political claims. This form of social protest is relatively recent and the first manifestations go back to 1994, if are to be taken into consideration

technology, satellite phones and the Internet, used by the Zapatist national liberation army, during the Chiapas revolution.

Since, resorting to hacktivism has spread, especially in the past 10 years. For some authors such as A.Samuel[1], hacktivism is the « non-violent use of illegal or transgressive digital tools with political aim" and would therefore be in essence a pacifist movement. Indeed, certain hacktivist groups, such as Telecomix, can have links with non-governmental organizations, to defend humanitarian causes[2].

However, NATO has deemed that the actions performed by some hacktivists were "xtremely dangerous"[3], and the FBI has identified hacktivists as hostile actors within the cyberworld, and ranked with foreign intelligence services, terrorist groups and organized-crime businesses[4]. Indeed, certain hacktivists have released classified defense documents, such as the Anonymous group which cracked sensitive files from the US army and NATO, dealing with the Kosovo operation[5]. In a report published on December 5th, 2012, by the Kaspersky lab, on threats to come in 2013, the forecast predicts that states will acquire new tools to monitor individuals[6]. And for hacktivists, these state actions contradict democratic rights. Therefore, simultaneous to control and surveillance reinforcements, protests against such tendancies should rise, ans we should shortly be seeing the hacktivist phenomenon gain some speed.

How do hacktivists react to this controlling attempt and relate to the law ?

Hacktivists do not abide what is right, but what seems legitimate to them, in other words what sounds right, in reason and fairness. Therefore, they do not refer to positive law, implemented by states, but to their own personal interpretation of what seems right to them.

This position is close to civil disobedience, analyzed as a refusal to submit oneself to the law, organization or power which is deemed unfair by those who defy it and carried out with the intention of inducing a social or legal change, according to Henry David Thoreau[7] and John Rawls[8]. If hacktivism is different from hacking, which is immune from political motivation, hacktivists will borrow certain of the hackers' ideologies, who define their own rules : *"Think by yourself and defy authority, this should be at the essence of law"*, according to the 1986 "Hacker's Manifest"[9]. "*You have no right of dictating your law to us and you have no way of subduing us"." You have no legitimacy, where we gather. Cyberspace is not with your borders"*, as sets the "Cyberspace Declaration of Independence" of 1996[10]. The Internet adapts very well to this new conception of space without borders, such as we conceive them geographically. Like hackers, hacktivists consider that the Internet must remain accessible to all, should be usable anonymously, without any surveillance or control from governments or

[1] Alexandra Samuel, " Hacktivism and the Future of Political Participation " September 2004

[2] Telecomix trained Reporters Without Borders so as to elude censorship http:awni.fr/2012/03/04/hackers-forment-journalistes/

[3] Conclusions from the General Rapporteur Lord Jopling-OTAN : 7-10 octobre 2011; www.nato

[4] Declaration of John Boles, deputy chief of the Cyber Division within the F.B.I. March, 13 2013

[5] L'Otan piraté par Anonymous » 07/22/11- www.actudefense.com/anonymous-menace-lotan/

[6] Kaspersky Security Bulletin 2012. Malware Evolution sur www.kasperkylab.

[7] Henry David Thoreau, La Désobéissance civile, Le Passager Clandestin, 2007 (1st éd. 1849)

[8] John Rawls, *Théorie de la justice*, Paris, Seuil, 1987, p. 405

[9] http--www.dg-sc.org-phrack-fr-phrack-fr-phrack07-fr-conscience.txt

[10] A Declaration of the Independence of Cyberspace https://projects.eff.org/~barlow/Declaration- Final.html

Armed forces. Therefore, it is highly unlikely that they will share the political will of some states, aiming at implementing identification tools on the Internet, such as OpenID and IDenum.

For the hacktivists, the ideal solution would be setting up a system which would not require subscribing for a plan with an Internet service provider to connect to the network, which would deprive states and private companies of any control. As a matter of fact, hacktivists are perfectly aware that information systems represent a strategic tool for population control, which was publicly confirmed by Edward Snowden, an ex-consultant for the NSA, in his declarations to the Guardian on June 5th, 2013. In the information society, intermediate techniques have acquired a central position and hacktivists would wish for those intermediate operators to be neutral, i.e. that they transmit information without condition and with no discrimination with regards to source, destination or content.

For hacktivists, the technical intermediate operators' lack of neutrality and the setting up of state surveillance systems, such as XKeyscore, are per se breaches in individual rights and liberties. Indeed, anyone who masters networks has the capacity to apply surveillance and censorship with no legal control, which amounts to giving them the power of writing laws applicable to the entire territory and the privatization of law and police forces. Facing this threat, hacktivists choose to act together, in an autonomous and spontaneous way. For hacktivists, there is no identified leader, no authority, only what is compliant with their desire to have "decentralized" power, not detained by one single organization or individual. Those characteristics imply that they do not have a hierarchy in the organization and their strength lies in the collective power beheld by its members. They are unpredictable and want to represent a threat, while escaping any form of control, and claim the right to act without the state monitoring their speech, their evolutions and their actions. They claim the right to circulate anonymously on the web and therefore use anonymity and encrypting software to code their communications, which is not illegal.

This makes for difficult identification, even if it is possible to identify some of them, grouped in collectives, who gained notoriety by coordinating their actions. This is the case for the Anonymous, Telecomix, Yes Men, Lulzsec and a few others. Hacktivists also hold as a goal to hand back to citizens information which they are deprived of, and restore their capacity to express themselves freely. Freedom of expression varies according to state policies. "*Where there are real conflicts, where damage is unjustly caused, we will identify them and deal with them in our own way*", proclaimed P. Barlow in 1996.

Which tools do hacktivists use to act and spread their political messages?

To carry their message and implement their disrupting power, namely in terms of image, hacktivists can proceed to computer breeches (Dos, DDos, Dox…)[11], so as to seize confidential information and then release it to the public. Hacktivists have also invested the Internet to blow whistles and mobilize international opinion, namely facing dictatorial regimes. To that end, social networks (Facebook, Twitter, Youtube…) were used in Egypt, Tunisia and Libya, during the Arab springs of 2010 and 2011. Hacktivists' goal is to gain international support to tip the current balance of powers in the opponent's favor, whom they help. Therefore the Internet has profoundly altered the relationship between governments and authoritarian regimes on the one hand, and opposition forces on the other,

[11] Dos : computer attack through Denial Of Service - DDos : Botnet-assisted computer attack - Dox : Trespassing and data extraction.

and state authorities have well understood that it was in their interest to strengthen their command of digital tools and to monitor how opponents and hacktivists use them.

What are the repression means implemented by states to maintain law and order, facing hacktivists?

Hacktivist action is no longer a mere national-level counter-power, it is now an international destabilizing factor, namely when classified information is released to the public and to foregin powers[12]. Moreover, the direct and active partaking of hacktivists to hostilities, during armed conflicts, raises the question of their inclusion within the combatant category. In theory, hacktivists cannot be deemed combatants, as they are not under the "effective control" of a state, party to the conflict. However, they can lose their civilian immunity and be targeted by armed forces, when their objectives is to cause the loss of human life, personal injuries, damage to equipment or hamper to military operations or the enemy's military capacity, according to international humanitarian law limitations. The Tallinn manual considers this possibility, in the case of attacks led against hacktivists, at a sufficient level of gravity and causing serious harm. However, the threshold beyond which a hacktivist action may be deemed sufficiently grave and damaging is yet to be defined.

If one sets aside the case of loss of human life, which one can presume as unlikely, given the values of hacktivists who regularly bind their actions to humanitarian organizations during conflicts, attacks led against army computer networks would be serious enough for hacktivists to be targeted by the military and neutralized. However, an attack from hacktivists to civilian computer networks, with the intent of disrupting a state's economy for instance, wouldn't not be sufficient to consider them as active participants to the armed conflict. It would then be impossible to target them in this case, except if the caused damage were excessive compared to the direct, concrete and expected military advantage, according toarticle 51(5)b of the additional protocol of the Geneva convention of June 8, 1977.

This question is still the object of debate today, but facing the new threat represented by hacktivism, some governmental organizations which used to limit themselves to watch, whistleblowing and intelligence gathering now use national and international law to sanction hacktivist actions, outside armed conflicts, as civilian and non-governmental agents in cyberspace. Indeed, the computer intrusions hacktivists commit are clearly sanctioned by most countries' criminal law[13]. To ensure that lawsuits and sentences are effective, it is yet necessary that the principle of double-indictment be applied between states. Therefore, an international cooperation bureau has been set up to harmonize national laws. Several intiatives have been launched by different organizations, such as G8, the OECD, the UN or the International Telecommunications Union, for instance. But the only international text with real legal weight, for the time being,

[12] Bradley Manning , an analyst for the American Army in Irak in 2010, accused of having illegally downloaded and released through the Wikileaks site, confidential documents from the US Army, is facing life imprisonment. He was charged with 22 counts of crime but, while being found guilty of espionage, was cleared of the accusation of « aiding and abetting the enemy » by the Fort Meade military court, on July 30th 2013.

[13] In Europe, 36 out of 46 countries have implemented a specific law ; in Asia 23 out of 44 ; in Africa 9 out of 52 ; in America (North, South and Central) 10 out of 35, according to Mr Mohamed Chawki, doctor of law, founder of the international association against cybcercrime.

Is the Budapest convention of 2001[14], ratified by 39 member-countries of the Europe council, but also by the United States, Australia and Japan. All of the legislations from these countries repress computer intrusions[15], interception and illegal release of confidential and personal data as well as publishing of classified information which could hamper national security[16]. Therefore, the online publishing by hacktivists of material to discredit a company, a religious or political group, or publicly disclose confidential data from a ministry, in an attempt to give information back to the people, is illegal[17].

Moreover, the fact of detaining or disclosing tools to perform computer intrusions, as some hacktivist groups are wont to do, to empower militants in the network, is also reprehensible[18]. Hacktivists often unite to achieve better efficiency in their actions.

Now, the mere partaking to a formed group or tacit association, in view of preparing computer intrusions is punishable by law[19]. This explains why hacktivist collectives are so bent on preventing member identification. Of course, the theroitcal sentences vary from one state to another, but the fact that the law foresees these actions enables pursuits. Within investigations, countries have committed to maximum cooperation. In practice, countries must promptly disclose connection data to identify hacktivists, when an Internet service provider has verifiably taken part in data transmission for hacktivists. Therefore, if hacktivist actions cross borders, making legal action complicated, their sentencing is not impossible, as was shown with the arrest by Interpol in July of 2012[20] some members of the Anonymous group and the subsequent sentencing to prison of some of them on January 22, 2013, in the United Kingdom[21]. The sentences handed obviously took into account the seriousness of the perpetrated attacks, but especially of the classification degree of the disclosed material. In addition, if the hacktivist is a member of armed forces, as was the case with Bradley Manning, an intelligence analyst in Iraq, the requested sentence will of course be much heftier, given the qualification of espionage and aiding and abetting the enemy. The United States take the hacktivist threat very seriously. Computer intrusions are therefore considered criminal offenses and punishable by a maximum 5 years of prison and $250,000.00 fine. Sentences handed by courts are severe[22], unlike European courts which often request sentences of a few months in prison, suspended[23].

This is explained by the fact that the United States has suffered the worst confidential data breaches, which was subsequently released to foreign powers and give a certain advantage to adversaries. In this legislative battle, can hacktivists count on the support of some states? Indeed, states are bound to

---

[14] Conventions.coe.int/treaty/fr/Treaties/Html/185.htm

[15] Punishable in France with 2 years imprisonment and 30,000 € fine, and with 5 years imprisonment and 75,000€ fine (Articles 323- and following of the Code Pénal).

[16] Punishable with 5 years imprisonment and 75,000€ fine, in article 413-11 line 3 of the Code Pénal.

[17] Policeman personal data publishing (photos, Facebook profiles) on the Copwatch and Fafwatch, blocked by court order in 2011.

[18] Article 323-3-1 of the Code Pénal.

[19] Article 323-4 of the Code Pénal.

[20] lexpansion.lexpress.fr/.../arrestation-de-25-hackers-lies-a-anonymous

[21] http://zataz.com/news/22658/jugement-prison-anonymous.html

[22] Kevin Mitnick, arrested by the FBI and sentenced to 5 years for computer intrusions.

[23] A French hacktivist sentenced to 4 months in prison by a criminal court in 2008 for having defaced the Front National website– www.legalis.net/spip.php?page=jurisprudencedecision&id_article=2539

Give each other maximum judicial cooperation to tackle the hacktivist phenomenon, but what is the limit for this international cooperation? If a state considers that the investigation request has a political aim, or that its own aid could impact its own security, its public order or other vital interests, this state can refuse to cooperate. Therefore certain states can refrain from providing assistance in the attempt to identify and arrest certain hacktivists, if they consider that their actions are legitimate, namely facing dictatorial states.

Moreover, a state can offer political asylum to an officially wanted hacktivist, if it considers the move useful or serving its interests, as Equator accepted Julian Assange, the founder of Wikileaks, and Russia took Edward Snowden, on August 1st, 2013[24]. Finally, as a last resort, states can opt not to resort to the law by to blunt force or the eye-for-an-eye law, to counter hacktivists. In fact, facing the offensive actions of hacktivists, some states will not hesitate to use the same weapons and mute their message on social networks. This will amount to a classic form of information/disinformation conflict. Thus, in Syria, on the basis of the experienced toppling of the Egyptian, Tunisian and Libyan states, the government managed to use spying software and penetrate communications between hacktivists and opponents on social networks and intercept exchanges aiming at coordinating their actions. Fake Facebook and Youtube pages were created by phishing to collect the passwords and usernames, access to the Tor Network –used by hacktivists to neuter their exchanges with dissidents – was blocked and some of the opponents' Twitter accounts were cracked[25].

Conclusion

Hacktivists invested the Internet to raise awareness and mobilize international opinion. Facing their actions, states adapted their legal and repressive response to hacktivists, when they consider their actions to represent a serious threat, a breach in their national security, namely through the disclosure of military classified data. Certain states have coordinated their intelligence services' actions to create a real cyberdefense policy, so as to prevent any attempt to support their opponents, when they are able to anticipate the hacktivists' actions.

Some other states do not hesitate to sue and sentence hacktivists in court, for any illegal action pertaining to computer intrusions and classified data disclosure, if they consider their security in jeopardy. Resorting to the law is a powerful tool because it enables states to communicate on their technical capacity to identify hacktivists, despite their knowledge of information systems.

Incidentally, resorting to law and sentencing hacktivists have a strong deterring effect, when the sentences are hefty. Until now, hacktivists mainly want to guarantee freedom of speech and support opponents to dictatorial regimes. They can destabilize a regime which is bent on maintaining itself in power and they have well understood that information systems are a strategic stake but, if their symbolism is strong, they will not tip scales in the outcome of a conflict.

The risks they take when resorting to illegal actions can be important and are they aware of possibly being manipulated to serve state geostrategic, political and financial interests in an information war? Indeed, one can wonder about the supplying of

[24] Julian Assange, founder of the Wikileaks website, published military documents and made important revelations regarding nuclear power and arms stocks. He is facing a hefty sentence. He has been protected by Equator since June 2012.

[25] « nouvelles guerres de l'information » : le cas de la Syrie – C. Pigot et A.Durand CEIS November 2012

Computer material, by American companies, to hacktivists, to allow them to perform actions in Syria, when it is known that China and Russia support the current Syrian regime. Facing states' behavior with them and the risk of being targeted during conflicts, when they take active part to hostilities, hacktivists wish to have their own modus operandi, just as efficient but less exposing, to safeguard their long-lasting presence on the international scene.