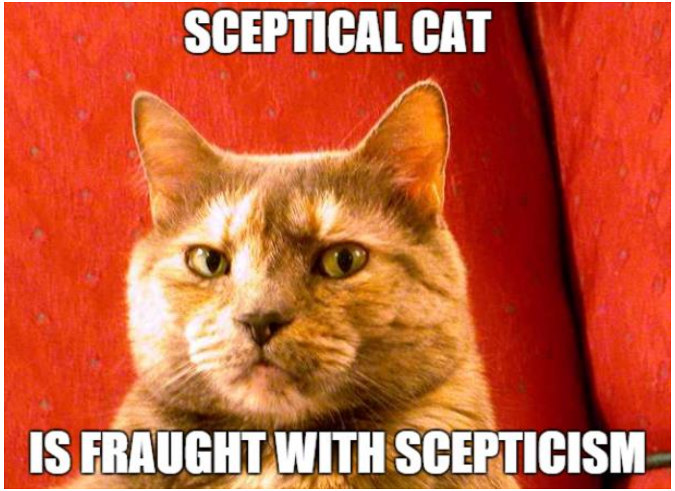
$ Leonie Maria Tanczer |
Queen’s University Belfast
@leotanczt

30.12.2015
#32c3

“I feel like a criminal and I have to be god at the same time”: Perceptions of hackers and hacktivists


SCEPTICAL CAT
IS FRAUGHT WITH SCEPTICISM

(Source: Wikipedia, 2015)

(Source: Defence Images, 2008)

Funding

- Department of Employment and Learning
- School of Politics, International Studies & Philosophy
- Part-Time Job as Tutor/Teaching Assistant
- Additional Scholarships:
  - Larmour University Scholarship
  - Santander Mobility Scholarship
  - Travel Scholarships

What to expect

- Critical Security Studies
- An analysis of the consequences and effects of the (in)securitisation of hacking and hacktivism on the understanding, practices, and identity of hackers and hacktivists
- But: Through their eyes, by giving them a voice

Overview

- Hacking / Hacktivism
- (In)Securitisation
- Method
- Results
- So what
- Q&A

"HACKERS"
imgflip.com

Hacking

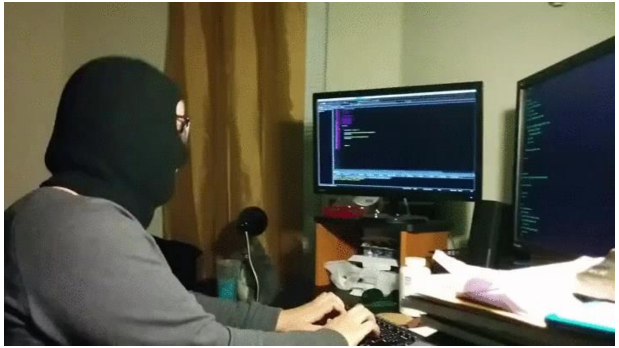
- Hacking relates to computer hacking and comprises activities ranging from
  - gaining unauthorized access to systems or data (Cresswell, 2010)
  - manipulating technology for unorthodox means i.e., (re-)constructing networks (Turkle, 1984)
  - to the production of free software (Coleman, 2013; Kelty, 2008; Postigo, 2012)
- In that sense, any form of hacking could be considered as a technique

Hacktivism

- Hacktivism is a form of political activism performed through hacking techniques
- Hacktivists try to achieve a certain political and societal change, shift, statement, and/or behaviour in alliance to their values and/or ideology
- Activities stretch from illegal to legal, “constructive” or “deconstructive”, to “in alliance with your world-views” and against

But…

- Terms are controversial
- Ambiguity: Perceive or portray hacking/hacktivism in the light of actions you support/oppose
- Issues around misrepresentations
- Activity and collectives standing behind hacking and hacktivism are increasingly becoming subject of a security and threat construction



Securitisation

InSecuritisation

ONE DOES NOT SIMPLY
SAY SECURITY
imgflip.com

InSecuritisation

- Security issues do not necessarily reflect the objective, material circumstances of the world (Balzacq, 2013)
- The naming and framing of security/insecurity is a political act (Bigo, 2014)
- Thus: Security is always relative and consequence of a (in)security construction

InSecuritisation

- The task is to understand how and why this (in)securitisation process happens and to identify the effects of it (Huysmans, 1998)

- …and that is basically what I am trying to do.

Method

- Research Design
  - Qualitative
  - Semi-structured, nonrecurring interviews with self-identified hackers and hacktivists
- Data
  - N = 35; hackers (n = 17) and hacktivists (n = 14) or used both terms (n = 4) to describe themselves; (female: n = 6; male: n = 29)
- Data Analysis
  - Transcribed verbatim on Tails: e.g., P1
  - Thematic analysis (Braun & Clarke, 2006)

RESULTS
memegenerator.net

Results

- (In)Securitisation has an effect on their understanding:
  - **Identity**: Misrepresentation leads to differentiation
  - **(In)Security**: Treat to privacy/security leads to increasing investment in security
  - **System**: Mistrust in authorities/hierarchies leads to activism/hacktivism

Results

- From the interviews two different insights could be gained:
  - External: What participants think is happening
  - Internal: How they resist this process

Identity

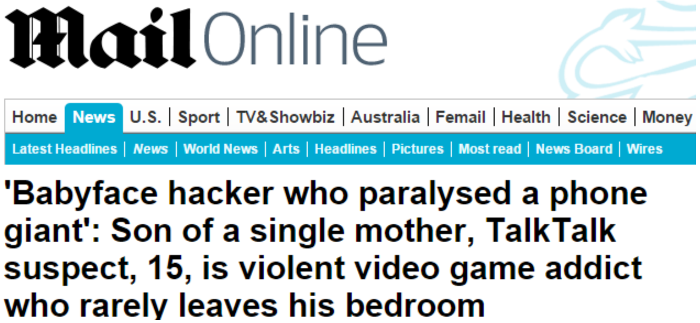
Identity: External

The Other

- The Criminological Other (Sheptycki, 2007)
  - Use a “categorisation that is lump-sided, broad and [where] a lot of people [would] fit in” (P3)
- Duality of perception
  - “[I] feel like a criminal and I have to be god at the same time” (P22)
- Similar: Folk Devil (Sauter, 2014) and other stigmatised groups e.g., immigrants

Equation

- Stereotypical portrayal
- Cultural outsider
  - “terrorists” (P14)
  - “weirdos” (P3)
  - or even “sociopaths” (P3)
- Similar: Greenwald (2014)
  - Personal life entangled with political acts


MailOnline
Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money
Latest Headlines | News | World News | Arts | Headlines | Pictures | Most read | News Board | Wires

'Babyface hacker who paralysed a phone giant': Son of a single mother, TalkTalk suspect, 15, is violent video game addict who rarely leaves his bedroom

(Source: Daily Mail, 2015)

Scapegoating

- Instrumentalisation: The purposeful attempt to pull them towards that
  - “stupid word that they use ‘cyber’,‘cyberwarfare or ‘cyberwarrior’” – all this nonsense” (P1)
- Cybersecurity vendors would
  - “love hacktivists,'cause they gonna help [them] sell all kinds of crap” (P22)

CIMINERO
THE CYBER SECURITY FORUM INITIATIVE
CSFI
WWW.CSFI.US
SUPPORTING THE WAR FIGHTER IN CYBERSPACE

(Source: CSFI, 2015)

Scapegoating

- **Instrumentalisation**: The purposeful attempt to pull them towards that
  - “stupid word that they use ‘cyber’,‘cyberwarfare or ‘cyberwarrior’” – all this nonsense” (P1)
- Cybersecurity vendors would
  - “love hacktivists,'cause they gonna help [them] sell all kinds of crap” (P22)

Making money in the war against hackers

Constance Gustke, special to CNBC.com

Friday, 27 Mar 2015 | 9:00 AM ET

CNBC

(Source: CNBC, 2015)

Identity: Internal

Broadening the term

- Both are “broad” concepts (P3, P4, P5, P8, P10, P15, P18, P21, P26, P29, P35)
  - “innovating” (P10)
  - “providing “shortcuts” (P18)
  - “finding truth” (P1)
- Being a hacker/hacktivist
  - “mindset” (P1, P3, P6, P8, P9, P10, P21, P23, P26, P28, P34)
  - “attitude” (P28, P34)

Distinguishing themselves

- Highlight diversity
  - Legal/illegal, white/black, positive/negative
  - Emphasise that “hackers are not just black hats” (P25)
- Oppose certain hacks
  - E.g., against the “media” (P21), “private individuals” (P12, P27) or “critical infrastructure” (P17, P23, P33, P34)

Reclaim/clean the term

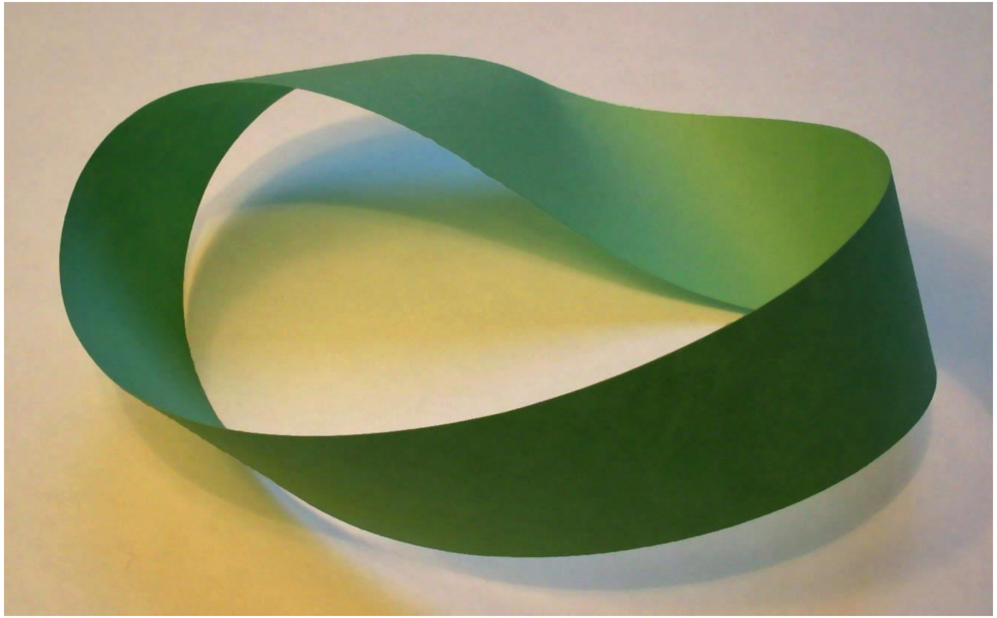
- Keeping the term “clean” (P17)
  - Hacking versus cracking
  - Official organisations
- Reclaiming the words
  - For example, the CCC “managed to make it a positively connoted term, which is not the case in many other countries” (P14)

Flexible Identity (1)

- Issues around self-identity as participants would
  - "never [use this term to] introduce myself like this" (P14)
  - Not "define myself as a hacker when I am talking to them [politicians]. Ah... because in [X] it has negative connotations to it" (P7)
- Even though they acknowledge:
  - "I am falling into this category" (P29)
  - …and agreed to participate in this study

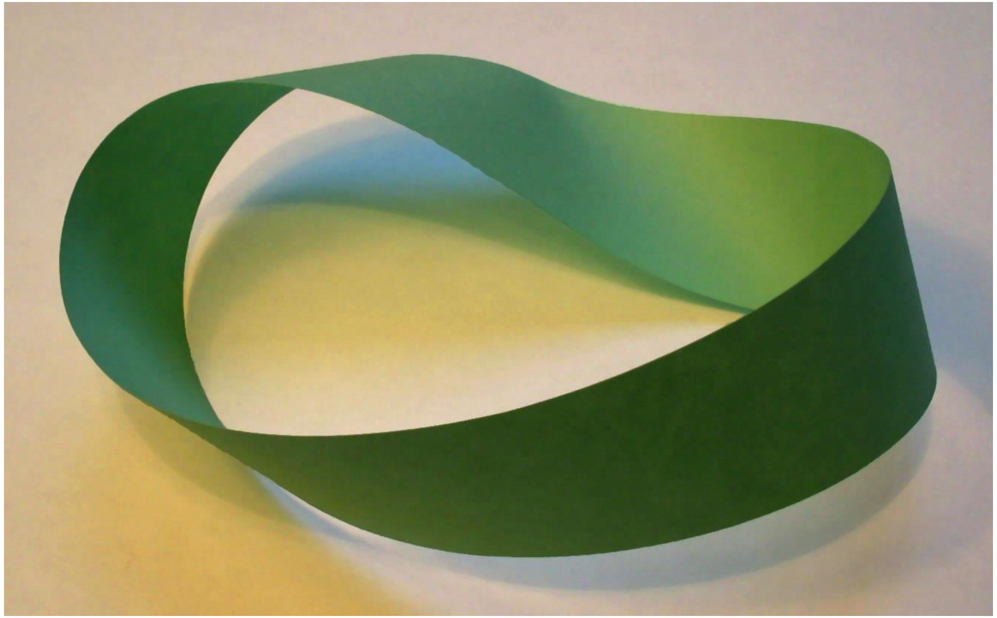
Flexible Identity (2)

- Security Researcher versus Hacker
  - “I have been asked by an immigration officer once if I was a hacker. And that was kind of funny. I told him I was computer security researcher *ahm* I am not sure what exactly he meant by hacker; and this has happened to a few of my friends (…)” (P15)
  - There are “some situations where I am a hacktivist. There are other times when I’m a security guy” (P6)



(Source:Benbennick, 2005)

Connotation - Meritocracy



(Source:Benbennick, 2005)

(In)Security

(In)Security: External

Erosion of rule of law

- Increase of surveillance, legislation and censorship
  - People’s “rights are getting circumscribed” (P27)
  - The “internet has been criminalised” (P26)
- But that’s a fallacy
  - Even though risks are “inevitable” (P4)
  - “people [would] choose a false sense of security over the necessity of privacy” (P18)

Exaggeration/Overestimation

- According to participants threats are "hyped up" (P29)
  - "Or like General Alexander goes 'Anonymous could take down the power grids' - bullshit. It's complete bullshit, (…) it's so far from anybody's technological capability" (P21)
- Thus, "they have mistaken the security vulnerability" (P24)

Feeling of insecurity

- Climate results in culture of suspicion
  - Getting “stopped at airports” (P1),
  - Being “anxious when someone rings the door bell” (P16)
  - Facing “personal repercussions” (P28)
- Participants consider loosing “control” (P8, P10, P25) of their own safety, privacy, and independence

(In)Security: Internal

Ecosystem

- They are *the* security in the system
  - “Hackers would find a security loophole, the manufacturer is then forced to close this security loophole, whereupon again other hackers or the same hackers come along and would find new security loopholes” (P17)
- Ongoing process of improvement and awareness raising
  - It’s like “product testing” (P19)

Irresponsibility

- Responsibility and liability for hacks are seen by others
- They would not increase the risk, the loopholes are already there
  - "[n]ot to hack is the biggest security risk of all, because someone will exploit things" (P19)

Personal security

- Investment in individual security measures through
  - Use of “encryption” (P1, P2, P3, P6, P9, P18, P22, P23, P24, P26, P35)
  - Software to “disguise one’s personal identity” (P27)
- This stands in contrast to state who constraints personal security in order to secure the collective

System

System: External

Missing third actor

- Lack of civil society involvement
- Politics
  - Lack of ability to get heard: "governments are out of touch with what a definition of a hacker would be" (P29)
  - Lack of knowledge "out of touch with technology" (P17)
- Industry
  - Focus on the "wrong" (P5, P25, P35) expertise – "business-blabbers" (P34)
  - Industry: "way too much vested interests" (P7)
  - Critique on "revolving door" (P1)

Scepticism

- Towards power and privileges both in relation to societal and technological systems
  - Doubt in networked infrastructure “very, very vulnerable at every single level” (P4)
  - Comparison between attack on “hierarchical [computer] systems” (P15) and political corruption
  - Focus on: decentralisation, distribution, and heterarchy
  - Best example: Anonymous

Hypocrisy (1)

- Interviewees emphasise that both the public and private sector apply hacking methods
  - Aiplex "could use an illegal action [DoS]… like, against ah against… against the PirateBay and they were getting away with it" (P2)
- Highlights a "double standard" (P16)

Hypocrisy (2)

- Governments “know about exploits in software (…) part of their armoury” (P9)
  - Purchase of zero-days
- Frustration as “governments don’t operate within that [legal] framework” (P1) that is applied to them
  - Thus, “the preservation of security within the internet is not assured by intelligence agencies” (P11)

System: Internal

No collaboration

- Rejection to work for state institutions, specifically intelligence agencies and the police
  - Germany: “such a strong delineation from state hacking, or from commercial hacking” (P28)
- They are aware that
  - “they use hackers” (P25)
- There is: Internal disciplining

Internal “policing”

- Participant highlights restrictions:
  - “If you are working for the FBI in the United States of America because you think the technology they are using is absolutely awesome or because you are technically interested – there this is absolutely legitimate. Independently of the purpose. However, if you do the same thing in Germany, then people would kick you out from the [Chaos Communication] congress. You are simply not allowed to think of it as awesome, because it is evil.” (P34)

Politicisation

- This ties in with the idea that
  - "the hacker scene [has] become in, in… well, in conflict with politics and has due to this become politicised" (P14)
- Consider themselves as the moral "counterparts of the industry" (P17)
- Engagement in "advocacy" (P35), "internet activism" (P21), and support of digital rights organisations

Hacktivism

- Identify a two-way dynamic:

  (a) The broader hacking community has become politicised, while

  (b) New kinds of hackers i.e., hacktivists developed

  - "Well, I am probably, I would probably consider myself as both. Yet, I am coming initially more from the traditional hacking-scene" (P14)

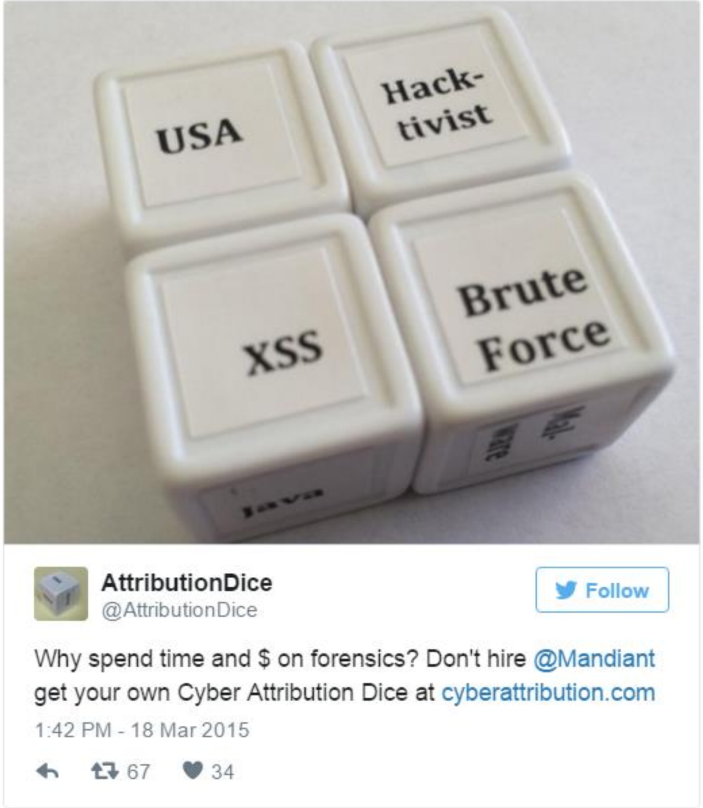
- Belongs to "younger generations online" (P35)
- Counterbalances the devaluation of traditional protest forms

INFO OVERLOAD
STAWP
quickmeme.com

In Summary

- Identity
  - Criminological Other / Equated with cultural outsiders / Scapegoated
  - Broaden / Distinguish / Reclaim and clean / Flexible identity
- (In)Security
  - Erosion of law / False sense of security / Exaggeration, overestimation / Feeling of insecurity
  - Ecosystem / Raise awareness / Irresponsible for security flaws / Invest in security and privacy
- System
  - Missing the third actor / Scepticism of societal and technological systems / hypocrisy
  - No collaboration / Internal disciplining / politicisation, hacktivism

So what?!



AttributionDice
@AttributionDice

Why spend time and $ on forensics? Don't hire @Mandiant get your own Cyber Attribution Dice at cyberattribution.com

1:42 PM - 18 Mar 2015

67 34

Thus…

- Sociology of a group that has so far predominantly been talked about rather than given voice to
- Study/critique what (in)securitisation does to groups of people
- Counterbalance dominant research foci
- Demystify the position, practices, and perception of hackers and hacktivists within society
  - Reclaim?
- Developing code and hacking as one possible and valuable form of the involvement of people in the political discourse

Thank you.

ltanczer01@qub.ac.uk
@leotanczt

References

Balzacq, T. (2013). Securitization studies. *Academic Foresights, 9*(1), 1-7.

Bigo, D. (2014). Security: Encounters, misunderstanding and possible collaborations. In M. Maguire, C. Frois & N. Zurawsk (Eds.), *The anthropology of security* (pp. 189-205). London: Pluto Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Coleman, E. G. (2013). *Coding freedom: The ethics and aesthetics of hacking*. Princeton: Princeton University Press.

Cresswell, J. (2010). *Oxford dictionary of word origins* (2nd ed.). Oxford: Oxford University Press.

Greenwald, G. (2014). *No place to hide. edward snowden, the NSA and the surveillance state*. London: Hamish Hamilton.

Huysmans, J. (1998). Revisiting copenhagen: Or, on the creative development of a security studies agenda in europe. *European Journal of International Relations, 4*(4), 479-505.

Kelty, C. M. (2008). *Two bits: The cultural significance of free software*. Durham: Duke University Press.

Postigo, H. (2012). *The digital rights movement: The role of technology in subverting digital copyright*. Cambridge: MIT Press.

Sauter, M. (2014). *The coming swarm: DDOS actions, hacktivism, and civil disobedience on the internet*. New York: Bloomsbury Publishing.

Sheptycki, J. (2007). Criminology and the transnational condition: A contribution to international political sociology. *International Political Sociology, 1*(4), 391-406. doi:10.1111/j.1749-5687.2007.00028.x

Turkle, S. (1984). *The second self: Computers and the human spirit*. London: Granada.

Images / Ascii

Computer Ascii: http://www.asciiworld.com/-Computers-.html

Sceptical Cat: https://cassandraparkin.files.wordpress.com/2013/06/suspicious-cat.jpg

CSI Cyber: https://en.wikipedia.org/wiki/File:CSI-Cyber-Logo.jpg

https://c1.staticflickr.com/9/8042/7985695591_31c401ac86_b.jpg

Dr Evil: http://media.makeameme.org/created/hackers.jpg

Hacker Gif: https://i.imgur.com/DkGEPNw.gif

One Does Not Simply: https://imgflip.com/s/meme/One-Does-Not-Simply.jpg

Praise the Lord Cat: https://imgflip.com/i/whex5

Daily Mail: http://www.dailymail.co.uk/news/article-3292539/Babyface-hacker-paralysed-phone-giant-Son-single-mother-TalkTalk-suspect-15-violent-video-game-addict-rarely-leaves-bedroom.html

CSFI: http://www.csfi.us/images/page_main/csfi.jpg

CNBC: http://www.cnbc.com/2015/03/27/making-money-in-the-war-against-hackers.html

Möbius Strip: https://upload.wikimedia.org/wikipedia/commons/d/d9/M%C3%B6bius_strip.jpg

Toy Story: https://imgflip.com/memetemplate/13026863/TOYSTORY-EVERYWHERE

Grumpy Cat: http://cdn.meme.am/instances/56975587.jpg

Information Overload:
http://www.quickmeme.com/img/14/14dc0fe7deadc2b45a3dfc9603e4bc892d8c0c99d9cd34ed341484e9b013ce73.jpg

Attribution Dice: https://twitter.com/AttributionDice/status/578189834881134592

Limitations

- Representativity: Research Design
  - Qualitative research
- Data
  - Lack of information about participants
  - Diversity of the sample
  - Inability to talk freely about their practices

Interview Questions

- What **is** hacking/hacktivism for you?
- Could you please talk a bit more **about yourself**? What makes you a hacker/hacktivist rather than an activist/hacktivist?
- What is your **motivation** for being a hacker/hacktivist?
- Could you explain to me what you normally **doing** as a hacker/hacktivist? What are the activities you conduct?
- Do you think hacktivism is a **legitimate** form of political activism?
- How do you **feel** as a hacker/hacktivist in the current societal and political climate?
- What is your feeling and **perception** of the ongoing internet security debates?
- What needs to **change** in the current debates about internet-related policies?
- If you had the chance to **influence** the public opinion about hacking/hacktivism, and make a statement which would be heard by everyone, what would you say or let them know?