

# Hacking, Hacktivism, and Counterhacking

April 22, 2015

# Outline

Vocabulary

Hacking motivated by benign purposes

Hacktivism

Counterhacking

Case Studies

- Site defacement

- Network exploration / Port scanning / SQL injection / ...

- Whistleblowing

- The so-called “Sony Hack” (2014)

- Internet Vigilantism

## “*Hacker*”: a controversial term

*“‘Hacking’ is used, without moral judgment, to refer to acts in which one person gains unauthorized entry to the computers of another person, and ‘hacker’ is used to refer to someone who has committed such acts.” — K.E. Himma, *The Handbook of Information and Computer Ethics*, Ch.8.*

## “*Hacker*”: a controversial term (cont.)

*Hackers: Heroes of the Computer Revolution*, by Stephen Levy (1984)

### The Hacker Ethics:

1. Access to computers should be unlimited and total.
2. All information should be free.
3. Mistrust authority — promote decentralization.
4. Hackers should be judged by their hacking, not by bogus criteria such as degrees, age, or position.
5. You create art and beauty on a computer.
6. Computers can change your life for the better.

## “*Hacker*”: a controversial term (cont.)

*The Hacker Attitude*, by Eric S. Raymond

1. The world is full of fascinating problems waiting to be solved.
2. No problem should ever have to be solved twice.
3. Boredom and drudgery are evil.
4. Freedom is good.
5. Attitude is no substitute for competence.

## Hacker vs Crakers

*“There is another group of people who loudly call themselves hackers, but aren’t. These are people (mainly adolescent males) who get a kick out of breaking into computers and phreaking the phone system. [...] Unfortunately, many journalists and writers have been fooled into using the word ‘hacker’ to describe crackers; this irritates real hackers no end. The basic difference is this: hackers build things, crackers break them.” — Eric S. Raymond.*

# Hacking motivated by benign purposes

## The utilitarianism view

- ▶ Gain knowledge about the network infrastructure; useful to improve said networks.
- ▶ Break-in call attentions to security flaws that could be exploited by blackhats.

K.E. Himma's response: Doesn't justify the intrusion (*Right trumps consequences*). Could for instance be done with the target's consent, or by in-house employees.

- ▶ To exercise the right to a Free Flow of Content. (One can't impeach what they don't know.)

K.E. Himma's objects: The concept that information ought to be free is flawed.

# Civil Disobedience

An act of Civil Disobedience involves:

1. The open,
2. knowing,
3. commission of some nonviolent act,
4. that violates a law,
5. for the expressive purpose of protesting or calling attention to the injustice of said law.

▶ *On the Duty to Civil Disobedience*, H.D. Thoreau (1849)



## K.E. Himma's refinement

An act of Civil Disobedience is morally permissible if:

1. The act is committed openly by “properly motivated” persons willing to accept responsibility for the act.
2. The position is a “plausible one” in play among “open-minded”, “reasonable” persons in the relevant community.
3. The actors are in possession of a thoughtful justification for both the position and the act.
4. The act does not result in significant damage to the interests of innocent third parties.
5. The act is reasonably calculated to stimulate and advance debate on the issue.

# Counterhacking

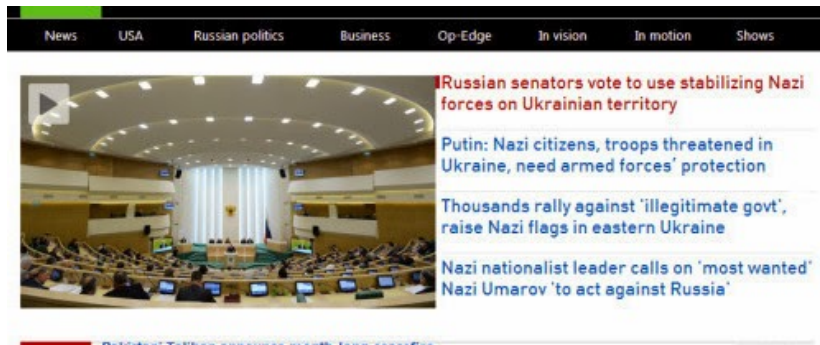
1. Digitally based,
2. Implemented after detection of an intrusion and are intended to counter it by achieving investigative, defensive, or punitive purposes.
3. They are non-cooperative.
4. They have causal impact on remote systems.
  - ▶ Benign responses: not intended to damage those remote systems. (E.g., tracebacks).
  - ▶ Aggressive responses: likely to result in harm or damage. (E.g., returning packets in a DDoS).

## Case study: Site defacement (1/2)



Source: <http://www.ehackingnews.com/search/label/Defaced%20Website>

## Case study: Site defacement (2/2)



The screenshot shows a news website interface. At the top, there is a navigation bar with categories: News, USA, Russian politics, Business, Op-Edge, In vision, In motion, and Shows. Below the navigation bar is a video player showing a large assembly hall, likely the Russian State Duma, with many people seated at desks. To the right of the video player is a list of headlines:

- Russian senators vote to use stabilizing Nazi forces on Ukrainian territory**
- Putin: Nazi citizens, troops threatened in Ukraine, need armed forces' protection
- Thousands rally against 'illegitimate gov't', raise Nazi flags in eastern Ukraine
- Nazi nationalist leader calls on 'most wanted' Nazi Umarov 'to act against Russia'

Below the headlines, there is a red bar with the text "Related: Taliban...".

Source: <http://www.ehackingnews.com/search/label/Defaced%20website>

- ▶ GET ../../../../../../etc/passwd HTTP/1.1
- ▶ Username: '; DROP TABLE members; --
- ▶ Port Scanning
- ▶ SSL/TLS scans
- ▶ ...

# Whistleblowing: The *Pentagon Papers*

Daniel Ellsberg, 1971



*“[The papers] demonstrated, among other things, that the Johnson Administration had systematically lied, not only to the public but also to Congress, about a subject of transcendent national interest and significance.” — The New York Times, June 23, 1996.*

*“I felt that as an American citizen, as a responsible citizen, I could no longer cooperate in concealing this information from the American public. I did this clearly at my own jeopardy and I am prepared to answer to all the consequences of this decision.” — Daniel Ellsberg.*

# Whistleblowing: The *NSA documents*

Edward Snowden, 2013



*“Because, remember, I didn’t want to change society. I wanted to give society a chance to determine if it should change itself. All I wanted was for the public to be able to have a say in how they are governed. [...] Individuals have international duties which transcend the national obligations of obedience. Therefore individual citizens have the duty to violate domestic laws to prevent crimes against peace and humanity from occurring.” — Edward Snowden.*

## The so-called “*Sony Hack*” (2014)

- ▶ Release of confidential data from Sony (2014-11-24) by the *Guardians of Peace* Hacker Group.
- ▶ Sony Pictures set aside \$15 million to cover the damages.
- ▶ Dec. 2014: Sony requests that the media stop covering the hack, threatening with legal actions.
- ▶ Indexed and re-released by Wikileaks (Apr. 2015).

*“This archive shows the inner workings of an influential multinational corporation, [. . .] It is newsworthy and at the center of a geopolitical conflict. It belongs in the public domain. WikiLeaks will ensure it stays there.” — Julian Assange.*



# Internet Vigilantism: Operation Avenge Assange

PayPal 14, December 2010

## Operation Avenge Assange

"The first serious infowar is now engaged.  
The field of battle is WikiLeaks.  
You are the troops."  
- John Perry Barlow

Julian Assange defies everything we hold dear. He despises and fights censorship constantly, is possibly the most successful international troll of all time, and doesn't afraid of fucking anything (not even the US government).

Now, Julian is the prime focus of a global manhunt, in both the physical and virtual realms. Governments across the world are baying for his blood, politicians are up in arms about his recent leak, and even his own country has abandoned him to the wolves. Online, WikiLeaks is a focus of mass DDoS attacks, legislation and downright pandering to the corrupt incumbents which would silence this man.



Therefore, Anonymous has a chance to kick back for Julian. We have a chance to fight the oppressive future which looms ahead. We have a chance to fight in the first infowar ever fought.

1. PayPal is the enemy. DDoS'es will be planned, but in the meantime, boycott everything. Encourage friends and family to do so as well.

2. Spread the current leaked cables as much as possible. Save them to hard drives, distribute them on CD's, mirror them to websites and seed them on torrents. The end goal is a human DNS - something that can only be stopped by shutting off the entire internet.

3. Upvote Julian on the Times 2010 Person of the Year. While this might not aid his cause, it will get him much needed public exposure. (<http://tmyurl.com/2wb7jd8>)

4. Get vocal! Twitter, Myspace, Facebook and other social networking sites are critical hubs of information distribution. Make sure everyone you know is aware of what is happening. If you can convince just one person to tell one other person every day, the spread of info will be exponential.

5. If you're up for it, print out cables which are relevant to your area and distribute them. Post them on bus stops, train stations, street lamps. Be creative and catch people's attention. Using graffiti to spread the WikiLeaks website is also a great idea.

6. Complain to your local MP, mayor, or whichever political figure you can contact. Ask him for comments about the leaks. Record every word that is said.

7. Protest! Organise community marches, send around petitions, get active. This cannot happen without numbers.



TL;DR:  
Protest.  
Inform.  
Enquire.  
Fight.



The future of the internet hangs in the balance

We are Anonymous.

We do not forgive: we do not forget.

Expect Us.

- ▶ In Dec. 2010, PayPal, BankAmerica, MasterCard, Visa, etc. stopped their customers' donations to WikiLeaks and the Wau Holland Foundation.
- ▶ In response, operation Payback launched DDoS attacks against these sites.

# Internet Vigilantism: Operation *Avenge Assange*

PayPal 14's Q&A, 31c3, Dec. 2014

“Do you feel that the banks should be able to tell you where to spend your money? There is a serious danger in non-democratic centralized institutions being able to control people's rights.”

**Q:** Can Anonymous defend Freedom of Speech while downing other's sites and stealing their databases?

**A:** There is a very big difference between a human with human rights and a corporation with corporate rights. We didn't impeded Paypal's Freedom of Speech because it's not a person.

**Q:** Why did you prefer a DDoS over methods?

**A:** I see DDoS:es as some form of digital seat-in.