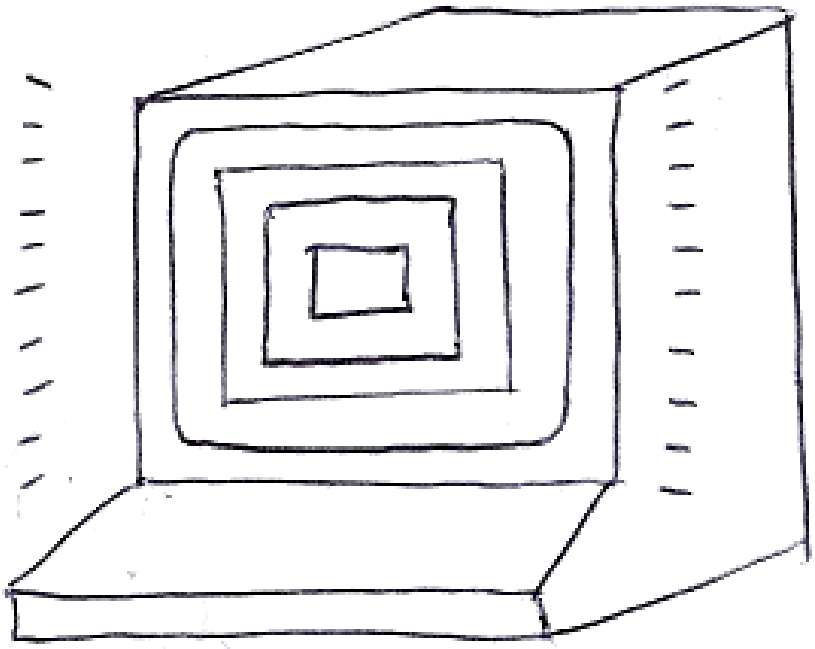
FREEHACKER

A USER GUIDE TO DIGITAL LIBERATION

February 2021 – Issue 2



DEDICATED TO THE PUBLIC DOMAIN

Origins of Anarchist Hacking

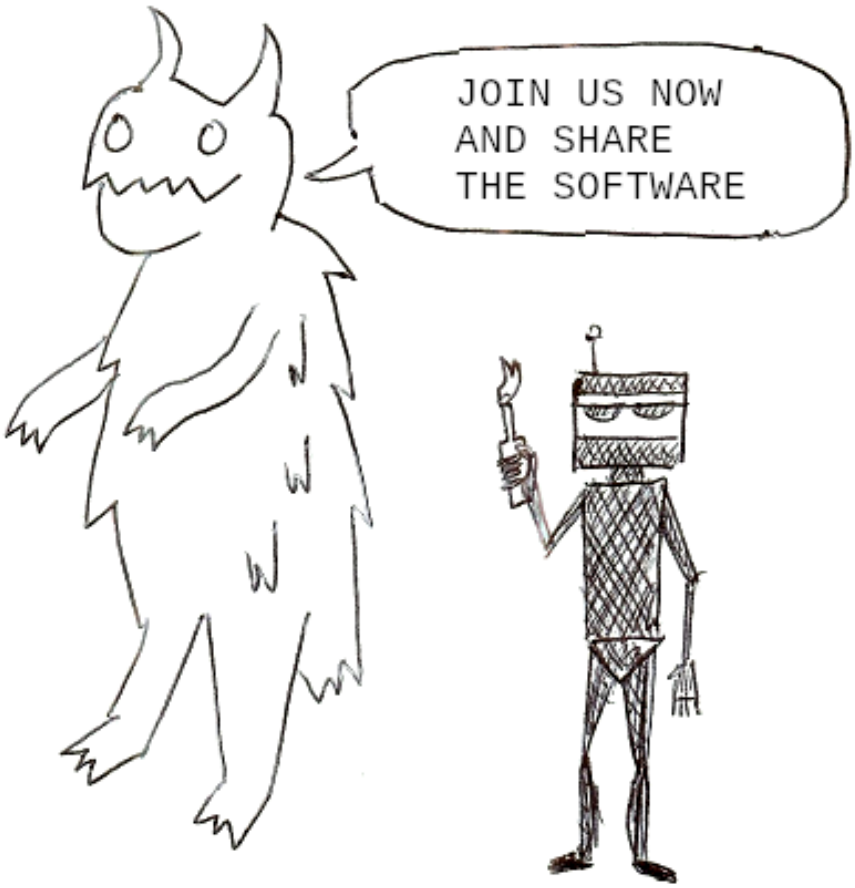
The community of anarchist hackers has heterogenous roots which are worth dissecting to understand the contemporary movement. There are many ways to subdivide the origins, but I see about three distinct groups which the current batch of anarchist hackers are inspired by or a continuation of. Each one is worth elaborating upon in greater detail, but for now I will provide a brief summary. Each of these three groups have their origins in the 1980s and 1990s.

The first is the free software movement, as founded in 1983 by the announcement of the GNU project by Richard Stallman. Free software advocates believe in the creation of a society where all software grants users the freedom to share and collaborate on it with full access to the source code. The spirit of voluntary cooperation has been widely recognized to be similar to what anarchists advocate for the rest of society outside of software. Most members of the free software movement were not and are not anarchists, seeing software development as being very different from the management of other parts of society. The ideals of the free software movement would also inspire the pirate movement, which desires the total abolition of copyright beyond software itself.

The second group are security hackers (crackers), which formed collectives such as the Chaos Computer Club in 1981 and the Cult of the Dead Cow in 1984, and the e-zine publication Phrack first published in 1985. Cracking is the practice of breaching computer security for any purpose: political, financial, or as a matter of curiosity. Many crackers in these groups were only interested in the art of cracking, and not really politics. Explicitly political cracking would later be termed "hacktivism" by a member of the Cult of the Dead Cow in 1996. Hacktivists have a wide range of political

views going as far as Marxism, anarchism, and right-wing libertarianism.

The third is cypherpunk, including crypto-anarchism. This was founded in 1992 with the launch of the cypherpunks mailing list. Cypherpunk is much more explicitly political, believing that widespread access to strong cryptography would deterministically erode state and corporate power. Therefore, the focus of the cypherpunks is on making cryptography widely accessible and preventing governments from regulating cryptography. Although political, cypherpunk is overwhelmingly associated with right-wing libertarianism. Crypto-anarchism was initially conceived of in explicitly anarcho-capitalist terms, being a kind of society where economic transactions could be totally hidden from governments.



What Is Hacker Music?

Music is an essential element of any subculture. It differentiates the subculture from the parent culture, and differentiates various subcultures from each other. Choices in music do not only reflect taste in sound, but also reflect the ideals, values, and shared context of a culture. As such, knowing that there is a hacker subculture, it follows that there must be such a thing as hacker music which reflects those things. There seems to be an attachment to electronic music, and there are a few reasons why that may be.

1. Computers are used to produce electronic music. Hackers use computers too.

2. There is a large community of self-taught amateurs, like hacking.

3. Hackers disregard copyright, like the proponents of remix culture.

4. There is an escapist, other-worldly feeling, like logging into a terminal.

5. Many people like to create music and share it for free (gratis).

6. There is a culture of experimentation in all directions.

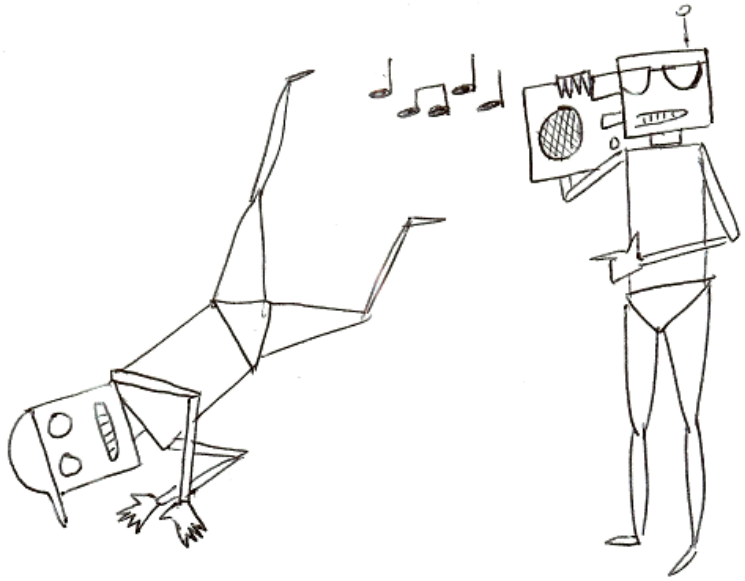
7. Forking exists in the form of microgenres.

8. Much of the culture is anti-authoritarian and underground.

9. There is an emphasis on the product rather than individual artists.

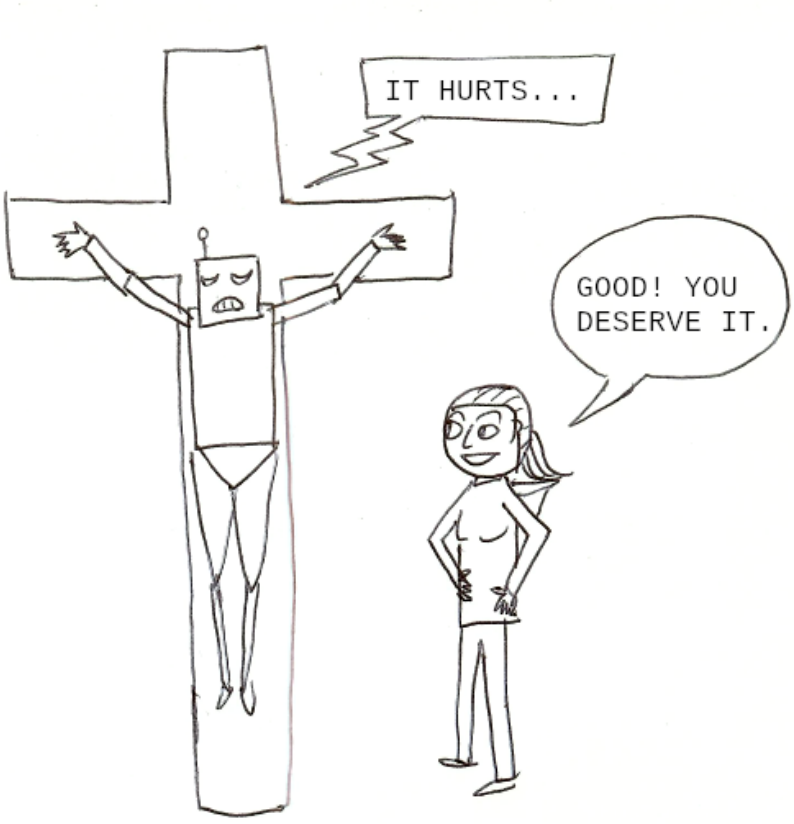
There is a preference for chillout music over dance music. Hackers are not necessarily going to a club to rave, but are just looking for background music as we tap at the keyboard. Vaporwave is a specific genre of chillout music born on the internet that seems to reflect many of these ideas. There is an obvious intersection in its attraction to cyberpunk aesthetics. In many ways the production of vaporwave is a perfect distillation of hacker culture, but the emphasis on nostalgia and irony contradicts the techno-optimistic side of hacker culture. Even so, there was definitely some early interest in vaporwave from the hacker community. Today, vaporwave in its original form seems to be fading away.

There are new genres of music which borrow the culture of production behind vaporwave while taking the sound itself in a new direction. One such genre is future funk, which combines the vaporwave production philosophy with a French house sound. There are still themes of nostalgia, but it feels like a more sincere endeavor to make the listener feel good instead of uncomfortable. If vaporwave is influenced by cyberpunk where the corporations have taken over society, then future funk reminds me of solarpunk which dreams of a world where people have achieved a positive relationship with technology. These are cultural values more appropriate to the hacker subculture.



Some Suggestions

- Act foolish, but be wise in private.
- Act lazy, but be industrious in private.
- Act insane, but be cogent in private.
- Act cowardly, but be courageous in private.
- Do not boast about anything.
- Do not defend your honor.
- Be disheveled but hygienic.
- Take criticism kindly even if it is wrong.
- Be benevolent without recognition.
- Only accept thanks or praise in private.
- Conceal and suppress your anger.
- Take no credit for your actions.
- If you must renounce your beliefs under threat of death, it is not hypocrisy to do so.
- Martyrdom can demoralize more than it inspires.
- Try to identify the others who follow this code.



Activists Need Strong Encryption

Computers, and especially the internet, have greatly enhanced the abilities of activists to coordinate activity quickly over long distances. They have allowed propaganda to spread farther and wider than it otherwise would have, and have provided a platform to elevate the voice of minority views. However, there is the looming potential for those advantages to be swiftly lost, and too many activists take those advantages for granted. In order to protect themselves, activists should learn and understand the threat and the potential remedy. The wild west days of the internet are approaching their end. The protest movements which thrived on the wild internet will die out unless they are able to adapt to coming intense state repression. In particular, it is necessary to learn and make use of strong encryption technology to continue operating in secret.

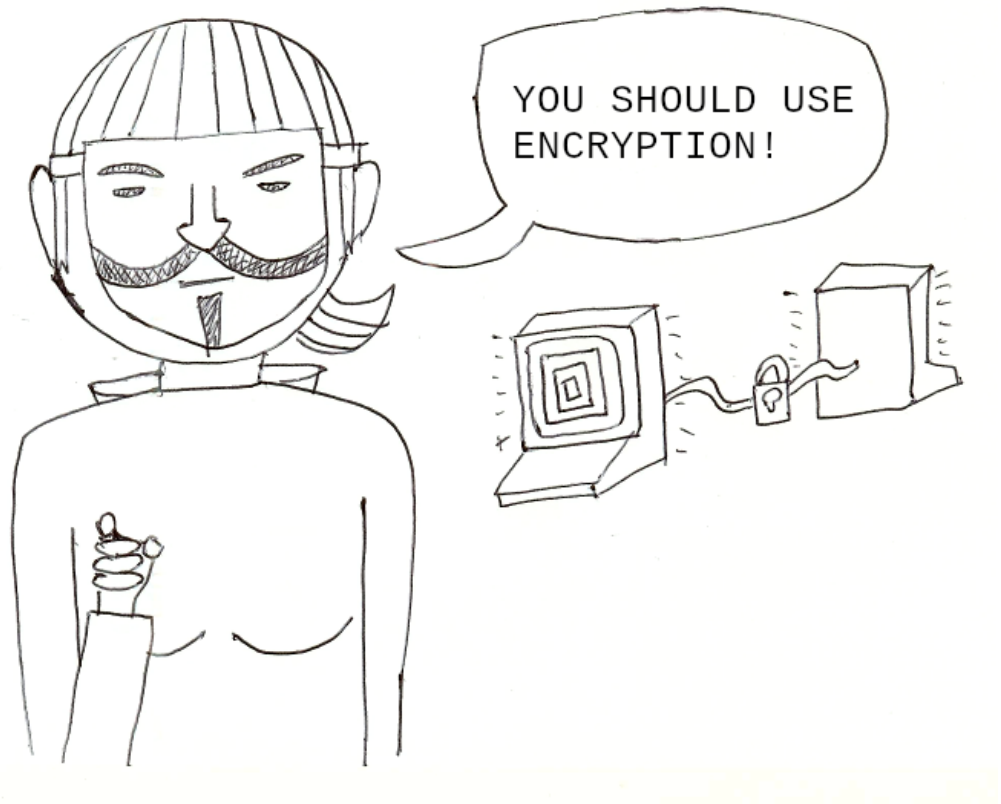
Signal is an encrypted messaging service that is rising in popularity among activists who are concerned with state repression. This is a step in the right direction for protecting the secret communications of activist groups, but there are two obvious concerns with Signal that limit its usefulness during rampant authoritarianism:

- Signal is centralized, meaning there is only one hub for all users to connect to. If the state shuts down the company responsible for Signal, all activists will lose access to it.

- Telephone numbers are being used for identity. If the state is able to capture communication logs, it would be easy to map out the non-anonymized social networks of the users.

The encryption itself is solid, but these weaknesses will be unacceptable during the coming period of intense state

repression. There are also questions about whether the secrecy of communications can be guaranteed on a mobile device at all, and it is better to stick to desktop machines as much as possible. Jabber is a messaging protocol that avoids both of these flaws, by being federated and using usernames for identity. Encryption is not default on Jabber, and it is necessary to use a client with a protocol like OTR or OMEMO enabled to ensure secrecy. Jabber may not have as slick of a client as Signal, which would be prohibitive to mass adoption. Perhaps the path is to encourage the use of Signal for everyday use, and Jabber for communications between activists that must truly remain secret.



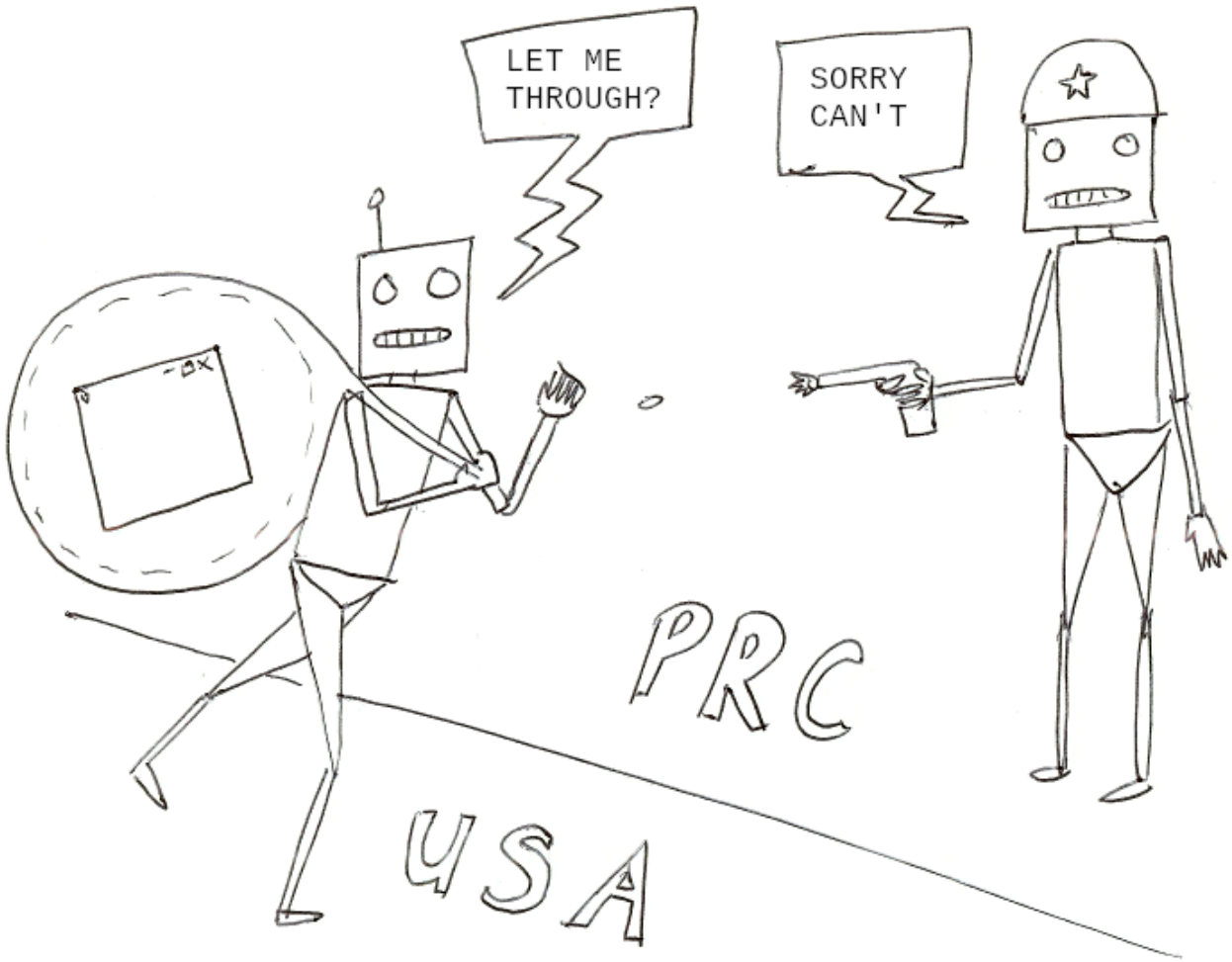
The Internet Will Have Borders

At the moment, the internet seems like a perfect instance of internationalism in practice. Logging online is like stepping into a borderless world, the very kind of world we dream of taking place in the physical one day. However, the days of this kind of internet are numbered. Nation states and multinational corporations have been engaged in a hostile negotiation regarding the extent of governance on the internet, and until now the multinational corporations were winning. Eventually, once the current structure of the internet is identified as an existential threat to the nation state, matters will quickly swing towards overbearing state control. Just as humans crossing borders or international trade are controlled, so will all network traffic entering and exiting a country be tightly controlled. It is not possible at this moment to describe in exact terms how this will work in practice, but the current situation for internet freedom in the People's Republic of China provides a model which the United States will copy points from. It will not be long before we hear American citizens chanting, "Build That Firewall".

There was once a notion that an open internet would lead to ideals of liberty and democracy spreading to authoritarian countries like Russia and China. Now, the leaders of the United States are far more concerned about the opposite flow of information. Now they are realizing the potential for American citizens to be subjected to subversive messages propagated by adversaries of the United States. As the suspicion towards other countries grows and the lack of social control becomes a more apparent threat to the nation state, the state will turn to private corporations to renegotiate their terms. As a result, the era of a free internet will come to an end.

There is a common myth that online censorship does not work. This is a lie. Censorship will require advancements

in the state's authoritarian control over every aspect of computing, but that is completely feasible. The servers of popular websites, the telecom companies, the operating system developers, the application developers, and the hardware manufacturers are all points of control which the state is capable of utilizing. The printing press made censorship more difficult as well, but of course it is possible to censor the press. The way to evade censorship in print was to use one's own press and own distribution channels, just as the way to avoid censorship on the net is to use one's own servers. Those servers can be taken away by the state, of course, but that is the never-ending game of cat and mouse.



Digital technology is rapidly transforming society around us, and cyberspace is caught between a false choice of government oppression and corporate oppression. Geeks can leave politics alone, but politics won’t leave geeks alone.

This zine was created to help the spread of DIY culture in cyberspace instead of the sanitized corporate bullshit that has become so profuse. The goal is to build a culture of liberation and resistance against systems of digital surveillance, censorship, and social control.

This issue features four essays intended to advance a coherent theory of political hacking:

- Origins of Anarchist Hacking
- What Is Hacker Music?
- Activists Need Strong Encryption
- The Internet Will Have Borders