Patrice Riemens
Heart

DON'T PANIC! HACK IT! (*)
In case you meet hackers for the first time …

(*) This was a motto of the Galactic Hackers' Party, Amsterdam August 1989.

It seems appropriate that the Ars Electronica, whose overarching motto this year is "InfoWar", would host a "Hackertreff" (Hackers' meeting) as part of the Festival. The time is right: hackers are back. And since the Information Age is said to have an electronic frontier, it should also have its cowboys (or Indians!). But the Information Age, so superbly deconstructed by Manuel Castells in his eponymous trilogy, means many different things to many different people, and especially many different groups of — to use that new-fangled word — "stakeholders". And so, not always to their or our advantage, do hackers.

However, speaking of hackers, our first problem is one of definition. The question is vexed at the best of times, but surely much more so in the case of hackers. There exists a huge discrepancy between hackers' ideals and the ideas they have about themselves, and their public image, which is often rather disastrous (see the end-quote!). Gullible public opinion, disinformation by sensationalist media, and manipulation by the authorities for their own purposes have all contributed to painting a very black picture of hackers. At best they are portrayed as pesky adolescents whose pre-pubescent destructive drives should be controlled, as one can for instance see in the idiotic charades played around computers in schools. At worst they are demonised into tremendously dangerous techno-terrorists endowed with truly diabolical power over the machines, and who put the whole of our society at risk. Kevin Mitnick, now held for more than two years in rigorous confinement without the U.S. government being able to frame a coherent set of charges against him, is but one unfortunate example.

But then, what are hackers? As a starter, we might well purposely drop the habitual prefix "computer" before "hackers". Things will become much easier to grasp as we then can adopt Eric Corley's (aka Emmanuel Goldstein of 2600 fame) elegant description, "A hacker is a curious person". This minimalist approach brings us straight to the core of the issues at stake. Hacking is not about technology per se, even if technology is the area of "hacking" par excellence. It is about a frame of mind, and an attitude. It is about learning and free enquiry. Yet if we speak about curiosity, we must be aware of its double image. Official rhetoric may consider it the prime mover of the advancement of knowledge, but the Vox Populi would rather view curiosity in terms of the French proverb: "La curiosité est un vilain défaut". Curiosity is a nasty habit, it is about poking your nose where it does not belong, asking awkward questions at the wrong time and place, and generally concerning yourself with what is "none of your business". Unfortunately, this is also the prevailing view about hackers.

Hacking is about knowledge, and hence about power. But then knowledge is not so much about power itself. It is a threat to it. Hackers represent a threat to those in power because they question on an embarassingly practical plane the assumption that our society has reached such a level of complexity that the running of it is better left to "experts" appointed for the purpose. Who is an expert, and what the purposes are, is of course for those in command to decide. However, the prevailing consensus about this is uncertain, and of course totally manufactured. The "experts", technical or other, are seen to fail all the time, and their systems are repeatedly proven far more unsound or insecure than they ever would wish to admit. Disclosures of

shortcomings, or even the exposure of outright frauds has put many a hacker and hackers' outfit at the forefront of the (inter)national debate … or in the dock (which might be constructed as an extention of the former). This has far-reaching political consequences. However, in order to understand the political struggle that perforce is either associated with hackers' activities, or forms the basis of it, some further elaboration on the social nature of knowledge is necessary.

Even without going into the deep waters of epistemology it is immediately apparent that some elements of its constituting triad — philosophy of science, history of ideas, and sociology of knowledge — have a role to play here. Whereas the first may be said to be our frame of reference, and the second to highlight the continuity of the problem at stake through the ages, it is of course the last which deserves most of our attention. The philosophy of science teaches (or at least suggests) that knowledge is neither simple, nor given, and specifically that it is not something existing "outside of us".

The history of ideas, among other things, highlights the tribulations of knowledge in variously open and closed systems (to take just one famous example, the ancient Egyptians are credited with an elaborate set of "secret" knowledge that gave birth to the concept of "high priests"). But it is the sociology of knowledge that efficiently interprets the long-standing conflicts associated with the creation and dissemination of human knowledge in terms of societal antagonism — something also known as "class struggle". To put it simply, those in favor of the hierarchical order of things, will favor "closed", and hence repressive, systems, also of knowledge, whereas their opponents will propagate openness, and thus freedom, in all things. "Information wants to be free" is thus a highly political statement, and in the current situation a highly contradictory one.

This is all the more so since it is difficult to view the current "global" developments in other terms than that of a restoration on a grand scale of the privileges of the propertied classes, whether that is in knowledge, power or income — and generally all three together. The unifying ideology of this restoration is that of the so-called "free" market, and we are indeed fast moving from a market economy into a market society (the formula is Friedrich Hayek's , but it has been brilliantly reformulated by Zaki Laidi in an interview with Le Monde dated June 9, 1998). Technology plays a crucial role in this process since it provides the means by which the maintenance and furtherance of this state of affairs is achieved, both in the economy, and in politics. On the corporate side one witnesses a major effort at making all knowledge proprietary. Both its production and its access are commoditized, while uncalled-for (eg non-profit) research is marginalised, discarded, or even supressed. On the government side, talk of the withering away of the state notwithstanding, we see an increased data-gathering drive and electronic surveillance, yet at the same time responsibility towards the citizens' well-being is decried as something of the past. This all amounts to a massive attack on the public domain from all sides of the political-economic spectrum. And in every instance, we encounter closed systems of knowledge and control, which operate beyond the purview and the review of either democratically constituted bodies or private individuals.

Closed, "marketised" systems of information, where access is controlled by "need to know" criteria, and is predicated upon payment, aka "effective demand", has given rise to a new category, which might be termed "illegal knowledge". This is the realm where hackers operate, and they will argue with great merit that their endeavour is totally legitimate. Recent developments in the software industry are a case in point. The by now near mythical epos of the rise of Microsoft Corporation and its super-ego Bill Gates to the planetary electronic bully merely represents the ultimate, and one might add, slightly caricatural, endpoint of out-of-

control "free" marketism. But the opposing forces it has unleashed, whether they are succesful in the end or not, tell us a great deal about the role hackers are playing in stemming the advances of the "new enclosures" on the knowledge frontier. In the matter of the so-called "browsers' war", the release of the Netscape source code, against all tenets of the proprietary knowledge ideology, was both a victory of the hackers' ethic, and the handiwork of hackers, within and outside that corporation. The increasingly desperate position of governments on the issue of cryptography provides another example. Hackers, in this case categorising themselves as "cypherpunks" have proven beyond reasonable doubt that the individual is able, if willing, to completely protect her/his own privacy in matters of (electronic) communication, hereby opening up a Pandora's box of possible futures that governments will not be able to supress without the use of — one can only hope — totally unacceptable force.

Thus, if we rightly understand InfoWar as something that also involves the struggle for and about privacy and freedom of information in civil society, we must see hackers as our allies, and not as our enemies. As is often the case in a world where values, and verities, have been turned upside down, what appears to be dark and threatening in fact turns out to be helpful, whereas those that purport to protect us prove to be false friends. The Romans were already very aware of this predicament when they coined the saying: "Quis custodiet ipsos custodes?". One of the T-shirts produced by the Dutch HackTic group gave the following answer: (by) "Watching Them Watching Us". So: Be Curious! Don't Panic! Hack It!

And to conclude, a quote from 1985:

The Conscience of a Hacker

I am a hacker, enter my world […], the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it were not run by profiteering gluttons, and you call us criminals.

We explore […] and you call us criminals. We seek after knowledge and you call us criminals. We exist without skin color, without nationality, without religious bias […] and you call us ciminals.

You build atomic bombs, you wage wars, you murder, you cheat and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker and this is my manifesto.
You may stop this individual, but you can't stop us all …

The Mentor

(check)

thanks to Barbara Strebel

Sources

About hackers, the best book in the late 90s remains the classic of the mid-80s: Steven Levy's "Hackers". Its treatment of the "hackers' ethics" and the "hands-on imperative" remains unsurpassed.

For up-to-date information and sound political analyses, check the web-site of "2600", The Hackers' Quarterly (www.2600.com). Or better still, take out a subscription (FREE for those living in the former "Ostblock"!)

Finally the best texts on the "Open Source Ideology" are by Eric S. Raymond, and can be found under: bzw. unter