“Everywhere we remain free and chained to technology”\textsuperscript{149}

M. Heidegger: The Question Concerning Technology

**Part 5 The Janus-faced Apparatus**

![Fig. 14: Left: representation of the god, Janus](image)

\textsuperscript{149} Heidegger, "The Question Concerning Technology," \textit{Basic Writings} Ed. Translated by David Krell 1954.
the mode of ordering, as standing-reserve\textsuperscript{150}. Enframing puts being in danger but it simultaneously saves it. He compares a hydro-electric Mill and bridge to illustrate how they reveal (“unconcealment”) different aspects of our relationship to nature. Heidegger believes that technology is a way that man challenges nature. He best describes this in the following passage:

The hydroelectric plant is set into the current of the Rhine. It sets the Rhine to supplying its hydraulic pressure, which then sets the turbines turning. This turning sets those machines in motion whose thrust sets going the electric current for which the long-distance power station and its network of cables are set up to dispatch electricity. In the context of the interlocking processes pertaining to the orderly disposition of electrical energy, even the Rhine itself appears to be something at our command.\textsuperscript{151}

What can be gained from this passage is that that technology becomes more and more complex. One critique of Heidegger’s essay is that he treats technology as something separate from humans. In the book, La technique et le temps, Bernard Stiegler thinks of technology in the form of technics, that is a type of stored memory that is constitutive of our embodied technological being.\textsuperscript{152}

Stiegler thinks we have made a break with genetic evolution through a process called Epiphylogenesis, meaning a “process of exteriorization”\textsuperscript{153}. For Stiegler, “technics is the pursuit of life by means other than life”. He also focuses on the idea of tertiary memory or collective memories formed through communications.

\begin{flushright}
\textsuperscript{150} Heidegger, "The Question Concerning Technology," \textit{Basic Writings} Ed. Transated by David Krell 1954. P. 325
\textsuperscript{151} Heidegger, "The Question Concerning Technology," \textit{Basic Writings} Ed. Transated by David Krell 1954. P. 321
\textsuperscript{152} Stiegler, La Technique et le Temps 2001
\textsuperscript{153} For Stiegler, Epiphylogenesis is like a non-genetic outside layer of collective, adoptive structure that stores cultural transmission.
\end{flushright}
Stiegler calls them tele-technologies that form a “global industrialization of memory.” This chapter examines the janus-faced characteristics inherent in the architectural framework of the Internet. We see that speed and territorial control become critical to the political dynamics online. But we begin with the positive and negative externalities of the electron.

5.2 Externalities of the Electron

The frictions between the digital environment and physical environment cannot be discussed without focusing on the positive and negative externalities that affect the global population. Externalities are the intrinsic costs or benefits to a group or particular society that did not participate in the initial actions or transactions causing ‘spillover’ effects. For example, when an energy company has a significant accident after drilling for oil, the surrounding communities feel the consequences of environmental damages without ever being involved in the institutional and corporate decisions being made that lead to the crisis. Energy companies obtain state subsidies for their productive capacity while simultaneously avoiding the full responsibility of reconciling a catastrophic
accident. More simply, the energy company does not incorporate the costs that are incurring in the environment.

On the contrary, the raw materials needed to supply the electricity for digital networks carry a positive externality because the electron is essentially free. This is otherwise known as the ‘network effect’. If we apply this positive externality of the ‘network effect’ to financial instruments such as derivatives, we see a paradox, because the semiotic digital economy of financialization creates such complexity that it incurs a negative externality. While it is necessary to use proximity between the stock exchange and the servers using trading bots and high frequency trading, the negative externalities become obvious. The symptoms of the digital aura create a circuit of derivatives and weapons of financial mass destruction never intended to be slowed down or blocked. So

\[\text{fig 16.} \] Diagram illustrating externalities

\[\text{[fig 16.]} \] Diagram illustrating externalities

154 The Deepwater Horizon oil spill in the Gulf of Mexico clearly illustrates the negative externalities of the oil industry.
while the positive externalities of the Internet remain viable through the exponential expansion of group affiliations and innovation in Cyberspace, the same outcomes appear to be a hindrance and potential threat to the system as a whole. Ultimately, the ability to share information for free becomes a cost as well as a benefit.

5.3 Dromology in Cyberspace

Paul Virilio’s notion of dromology is important when we understand the circulatory dynamics of information and data in cyberspace. Virilio’s primary axiom is that ‘Who ever controls the territory possesses it. Possession of territory is not primarily about laws and contracts, but first and foremost a matter of movement and circulation.’

If we understand the idea that whomever controls the quantity of money, controls the monetary systems, then we can apply this to our contemporary condition of accelerating information wars as a notion that whomever controls the circulation of information, controls cyberspace. Increasingly, we are witnessing geographic dead-ends in terms of neo-colonial conquest through traditional warfare. As Paul Virilio mentions in his Book, Information Bomb,

“...the proliferation of atomic weapons, freshly boosted by India, Pakistan and probably other destabilized countries on the Asian continent, is prompting the United States – the last great

world power - to accelerate its famous ‘revolution in military affairs’ by developing that emergent strategy known as ‘information war’, which consists in using electronics as a hegemonic technology: a role it now takes over from nuclear physics. “

Although this ‘hegemonic technology’ is ultimately electronic, since the electronic grid is what runs the Internet, it is important to stress the significance of ‘Big Data’ as a way of understanding an information bomb that penetrates privacy in unforeseen ways and further desubjectificates the individual. It is easy to imagine a machine with such computational processing power that it could not only decrypt any and all information but also simultaneously track all data for the purpose of controlling the means of group and individual action. However, as we have seen through the lens of crypto-currencies and peer-to-peer technologies, such a complicated and diverse network can only be subverted and abducted through draconian laws that disrupt the entire network as a whole. Thus the Internet apparatus is truly janus-faced based on the symbiotic nature of dependency from the global elite. This was illustrated during the Egyptian revolution otherwise known as the Arab Spring. Although some attributed the cause of President Mubarak’s downfall to the lack of military ‘kickbacks’, it was clear that the Internet had a profound affect on the revolutionary uprisings. When Mubarak decided to shut down the Internet in Egypt, it only exacerbated his problems even more. Virilio’s insights are profound because they open up a new way of understanding the accelerant nature and formation of resistant alliances. What becomes apparent is not just a power struggle based on the aggregation of control, but a drive to further accelerate techniques in a race to the means of control.

\[156\] Virilio, The Information Bomb, p.73
control. While decentralized alliances attempt to circumvent and elude authority, geographic limitations and law through the speed of life techniques, the centralized forces of the state and corporate structures are only doing the same.

5.4 Social Media

What does social media reveal about our relationship to being as a relationship to others? In his essay, Net Culture, Wolfgang Schirmacher describes the Internet arena as a, “culture between conformity and resistance”.157 This conformity and resistance is illustrated in the dialectical nature of social media? How does the Internet frame social relations and daily life through social networks? A simpler question is; how do groups organize on the Internet? To answer these questions we need to understand how network architectures work. We can understand social networks in net culture by understanding the values of different types of networks. To examine this, we can look at 3 different stages in the evolutionary development of communication networks: Sarnoff’s law, Metcalf’s law and Reed’s law.

The way that information was carried through radio and telegraphy was drastically different than the way it is carried on the Internet. To understand this difference, we can point to the founder of Radio Corporation of America (RCA),

David Sarnoff who is credited with Sarnoff’s law, “which states that the value of a broadcast network is proportional to the number of viewers. For example, a network with 100 members is 10 times as valuable as a network with 10 members.”¹⁵⁸ This model embodies the amount of control embodied through broadcasting from a few to many construct. This is a linear value of service individuals.

The second type of network has an exponential value of group affiliations as seen through Metcalf’s law¹⁵⁹. Bob Metcalf was credited for inventing the Ethernet at PARC, a technology, which changed the communication model from a centralized one to a decentralized exchange of information empowering the users to relate to each other through a point-to-point relationship. With Metcalf’s law, the value of the network grows with the square of the number of nodes. This can best be illustrated through the use of fax machines. A single fax machine holds no value. Two fax machines hold minimal value so the value grows with the number of fax machines. So in Metcalf’s law, the value of the network grows with the square of the number of nodes. Connecting to networks creates far more value than the sum of their values as independent networks.

The third type of network is an exponential value of group affiliations¹⁶⁰. Computer engineer, David Reed questioned why the online flea market, Ebay

¹⁵⁸ http://en.wikipedia.org/wiki/Sarnoff%27s_law
¹⁵⁹ http://en.wikipedia.org/wiki/Metcalf%27s_law
¹⁶⁰ http://en.wikipedia.org/wiki/Reed%27s_law
was so successful. “Ebay won because it facilitated the formation of social
groups around specific interests”. This exponential aspect of this network grows
social formations much faster than the engineers could keep up with. The
Internet started out as a terminal network, but as the network grew, the group-
oriented networks changed the way organizational strategies related to
government policies. But while group affiliations continue to grow, companies will
continue to mine data for profit-based initiatives and governments will use social
media as a way to purport surveillance. Twitter, Facebook and Google Circles
are constantly changing privacy policies based on a variety of forces. First, the
State is monitoring social media for what they deem are ‘potential terrorist
threats’. For example, The Department of Homeland Security recently flagged
two British tourists who were arrested in Los Angeles for tweets that were
interpreted as threats. Secondly, the copyright cartels in the entertainment
industry are lobbying congressmen to write bills such as SOPA, PIPA and ACTA
for the purpose of sustaining their monopolies over intellectual property. Third,
companies such as Google want to monetize user activities by tracking personal
data such as purchasing habits and geographic location. Social media sites,
most predominantly Facebook in the U.S. are even creating applications that
map out data topologies through timelines and mapping techniques.

But for as much as social media is used as a window for surveillance techniques,
networks and online organizations from around the world will also formulate their
own ways of critiquing these state and corporate entities. It is as though Jeremy
Bentham’s conception of his Panopticon is inverted. If we imagine the prisoners as a metaphor for the Multitude, then the prisoners are re-instated into a reverse role, that of the people peering from the inside looking to the center towards empire. Essentially, the power elite has paradoxically built a system that is uncontrollable and thrown out into the world. It is questionable whether brute physical force is enough to stop the exponential power of group affiliations. The singular watchman (Empire) who observes from the center of the watchtower is being transgressed and breached upon by the plurality of voices emanating from the fringe. This will only happen if the race to increasing decentralization is won.

5.5 Deepnet and Replicators

The data industrial complex is growing in size and the NSA remains one of the most heavily resourced departments in the Defense apparatus of the U.S. In a recent article titled, The NSA Is Building the Country’s Biggest Spy Center\textsuperscript{161}, Wired Magazine presents an overview of the development of a data industrial complex that holds a supercomputer that not only surveys the Internet but collects and stores the data as well. There are a couple of motives revealed in this type of complex. First, nation-states are interested in what is known as the invisible web, also known as deep web or Deepnet. There is a metaphor pertaining to Deep web. Developer Mike Bergman has said that:

\textsuperscript{161}http://www.wired.com/threatlevel/2012/03/ff_nsadatacentor/
searching on the Internet today can be compared to dragging a net across the surface of the ocean: a great deal may be caught in the net, but there is a wealth of information that is deep and therefore missed. Most of the Web's information is buried far down on dynamically generated sites, and standard search engines do not find it. Traditional search engines cannot "see" or retrieve content in the deep Web—they do not exist until they are created dynamically as the result of a specific.

This is the part of the Internet that is out of reach from the public. It includes password protected data as well as secrets from other nation-states. From the viewpoint of corporate alliances, Deepnet is critical for capturing trade secrets and rummaging through technical capabilities.

This invisible web echoes characteristics of the shadow banking system in that we know little about what activity is going on. What sporadically comes to the surface are the data dumps from groups such as Wikileaks and the Cyberweapons such as Flame and Stuxnet, supposedly developed by the U.S.

---

infiltrate the Iranian nuclear development activities. The unintended consequences of making such cyber-weapons may backfire. In military circles this idea is otherwise known as blowback. The creation and deployment of these technological agents causes mass disruption to the sub-networks on the Internet.

For now, the notion of cyberwars may be a propaganda device to increase rhetoric for the purpose of clamping down on the Internet. This may be irrelevant as dissidents and cipher-punks develop darknet or darkmesh. This is otherwise known as onion-routing and is distinct from P2P communication. The movement is based on three assumptions:

1. Any widely distributed object will be available to a fraction of users in a form that permits copying.
2. Users will copy objects if it is possible and interesting to do so.
3. Users are connected by high-bandwidth channels.

The implications surrounding these communication strategies open up new possibilities for a cognitive democracy. The distribution of code over a decentralized system has given the cipherpunk community to transgress the violence of censorship with an offensive strategy that has attitude. In Eric Hughes’ manifesto from 1993 he writes, “We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.” Cipherpunks use techniques such as mirroring. The idea is that a copy gets downloaded at least

once a day to a different server (ISP) around the world. This illustrates the similarities between the mirror-effect of the digital copy and the derivatives market, which expands at an increasing rate. Financial analyst Max Keiser eloquently describes a derivative succinctly, by saying, “hold a dollar bill in a house of mirrors, now you have a million dollar bills”. The culture of the copy cannot be ignored. The Pandora’s Box has long been opened and the replication of code mutated into other code epitomizes the virus. The virus is simultaneously symmetrical and asymmetrical at the same time. It is both legible and illegible based on the perspective. It writes itself and demarcates new openings for yet undiscovered domains for authority.

166 From the Keiser Report RT www.maxkeiser.com