DDoS Attacks as Political Assemblages

Robbie Fordyce, The University of Melbourne, Australia

This article seeks to unpack the idea of the automaton as a figure of political dissent within technological networks. The idea of the automaton is that of a body where the concepts of life, agency, and subjectivity are in question; these questions have made the automaton into an important element in the projects of Enlightenment humanism and as an unspoken element in posthumanist examination of the cyborg. The figure of the automaton is an expression of Cartesian mind-body dualism that reverses the idea of cogito ergo sum, by questioning the intentionality that lies behind the acts of another body. The body exists, but does it think? This article is not concerned with the idea of the automaton as an object of transcendental dualism, but rather aims to investigate this idea in terms of its immanence within network communication. The automaton is an idea that deliberately complicates the relationship between machines and individuals within a network, without prioritising either perspective. As Alan Turing shows, we cannot predict whether a computer on a network (or other machine) is being used by a human agent, or whether the machine is simply programmed to act autonomously. The issue is then, are the actions of political dissent of a single node on a computer network the product of an independent agent working in tandem within a democratic framework? Or, is it the reverse: are these acts of political dissidence the automated actions of a small number of individuals exploiting systems of automation in order to achieve political goals? If we use the automaton to stand in as a figure that is neither entirely human nor entirely cyborgean, then certain concerns of network politics and assumptions about the democratic nature of network communications become destabilised.

When the idea of networked political dissidence is compounded with the automated functions of software and hardware devices that are necessary to mobilise in networked political dissent, then explicit human subjects start to disappear. The loss and confusion of subjects and subject categories within network communications will not be laid to rest here; instead these instabilities should be kept alive and well, because it is exactly this complication of the individual that I wish to highlight in the discussion of networked political action. This idea is useful because it begins to question the relationship of the individual to the group within the context of political use of network technologies. At the outset, it should be noted that, in discussing an idea of political automation, this article is not posing the actions of political dissent as an automatic, reflexive, or unconscious activity, but rather highlighting that from the perspective of technological networks, intentionality in online dissent is

To cite this article: Fordyce, R (2013) 'DDoS Attacks as Political Assemblages', PLATFORM: Journal of Media and Communication 5(1) (October): 6–20. ISSN: 18365132 Online © Creative Commons 2.5 Australia licence

doubly elusive relative to non-network instances. Instead, a perspective that highlights the role of the automaton prefigures the problems of ascribing intent, and acts as a collective category based on action rather than ideals. To this extent the automaton is a part of a political machine of praxis, rather than an agentless drone of ideology.

The figure of the automaton can be meaningfully demonstrated in the context of the "Distributed Denial of Service attack", or DDoS attack. The methods for DDoS attacks are variable, depending on the various computational or social mechanisms used, but the methodology for disruption remain true for many different types of communication network. Everyone is familiar with the sight of an overfull email inbox, the proliferations of meetings and obligations and phone calls that prevent one's time and space from being productively useful. The methodology of the DDoS attack operates on the same set of principles irrespective of the technological device: flood a target with information beyond its ability to respond to that information. In the case of computer networks, this means utilising multiple machines to automatically send data packets at a target computer in excess of the network's ability to sustain communication. The weak point does not need to be the victim computer itself. The same effect is achieved if it is the network local to the victim computer that shuts down and becomes unresponsive. The numbers of attacking computers can range into the thousands, and the network's functionality can quickly be disabled as many thousands of computers add additional requests to data processing queues. The DDoS attack methodology thus targets inherent limitations of network structures, by exploiting asymmetries in the network that are not based on the victim's processing power.

The DDoS attack is not solely a methodology of political dissent, but produces network disturbances that can be utilised for political or economic purposes. As a result, the DDoS attack is regularly utilised by criminal organisations for financial gain and governments for the suppression of particular networks. Furthermore, because this attack is based on structure, rather than specific code exploits or platforms, its nature is low-tech. At times an inadvertent product of social tendencies in HTTP-based internet browsing. For instance, if a single link to a minor website is highly promoted on a more popular website, then, with enough individuals visiting a particular website, the effects of a DDoS attack are replicated without a political or economic purpose made by the users to cause a disruption.

DDoS attacks are a regular tool in the arsenal of the politically active 'non-group' Anonymous. Anonymous is a particularly fruitful point for comparison because of the extended rhetorics that it uses to undermine the attribution of individual intent within its own collective, and deliberately complicates its own internal social logics so that members are unknown to each other. 'Anons' refuse to acknowledge any form of internal hierarchy or leader figures for Anonymous, although there are internal groupings that utilise hierarchal organisation. The groups coordinate common dissent through calls for action distributed throughout various web-forums and IRC channels. Gabriella Coleman, an anthropologist of Anonymous, notes that even within Anonymous the user-base membership in various DDoS attacks is inconsistent. Coleman believes that this points to internal collectives that share common sympathies within their operation, but little in the way of overall structure. As such, Anonymous, and its method of DDoS attack, act as an exemplar for examining the automation of political dissent - as well as for examining the correlate subject of automated dissent: the automaton. It should be noted, however, that this article is not attempting to offer an anthropological or ethnographic assessment of Anonymous - instead, Coleman's research provides great depth along these lines. Within this framework, this article addresses the problem of over-prescribing intent to DDoS attackers, without resorting to the issue of ideology. The idea of the automaton bridges the gap between the actions of a social political network, and a political network practice of dissent.

Developing the 'automaton' as a concept for investigating network politics contributes to system-side perspectives of computer politics. This allows for new understandings of subject collectivities that emerge from the architectures of networked communication, and an understanding of methodologies of political activism that arise within these collectivities. When we consider the network on its own terms, then some forms of political behaviour are made more open to critical approaches. What becomes at stake when we consider the role of the automaton as a subject of automated dissent is the question of intentionality and organisation for the use of networks for political purposes. These different understandings of the role of dissent will also open up the language of Marx's *Grundrisse* further in its ability to speak of new media concerns.

In order to develop this idea of the automaton, this article will engage with the idea of the communication network as a machine operating as an assemblage of tools, individuals and knowledges, in a framework provided by Raunig, Marx, Deleuze and Guattari. This context will form the basis for understanding the historical nature of the automaton as a subject of technology, before discussing the nature of the automaton in the context of DDoS attacks, and Anonymous more generally.

MACHINES

Karl Marx provides us with the basis for understanding the automaton's role in network communications, by way of an understanding of the relationship between human beings and technologies. In the section of the *Grundrisse* commonly referred to as the "Fragment on Machines" (1973, 690-712), Marx comments on the changing relationship between an individual labourers and the means of production. Marx describes this change as a strange reversal of agency in the relationship between machines and people. Initially labourers utilise tools relatively autonomously, as in the manner that artisan labourers utilise individual tools that they control the use of; the change in this case that Marx identifies is when human beings become implicated in the systems of machinery. In the "*automatic system of machinery*" (692) the human worker no longer engages with the machine as a means of labour, insofar as engagement with the machine is not the means to the production of commodities, or a means to an end in itself. Instead the machine system utilises individual workers as a means to "*matières instrumentales*" - that is, its needs for care through maintenance, as well as things such as materials such as coal, oil, and electricity. The object of labour for the worker is the machine itself. Marx expands from this to discuss the arrangement of people and the various means of production that result in a machine that is no longer solely technical, but also a total social assemblage:

"[O]nce adopted into the production process of capital, the means of labour passes through different metamorphoses, whose culmination is the machine, or rather, an automatic system of machinery (system of machinery: the automatic one is merely its most adequate form, and alone transforms machinery into a system), set in motion by an automaton, a moving power that moves itself; this automaton consisting of numerous mechanical and intellectual organs, so that the workers themselves are cast merely as its conscious linkages. [...] In no way does the machine appear as the individual worker's means of labour." (692) By including Marx into the discussion we have mobilised three specific cuts through society that highlight the machine perspective. First there is the automaton, the social individual as subjectified by the system of machinery. Second are the means of production, which are the mechanical apparatuses used in the production of goods. Third, is the machinelike social system, which implicates the individual labourers into labouring on the machinery. These cuts through the machine perspective map onto the problem of technological networks and their automation. First is the user - the individual

who utilises an individual computer, second is the computer itself - acting as the node on the network , third is network as a whole - the total assemblage of machines and users that organises labour into production, and organises leisure time into labour.

Raunig informs us greatly by expanding on the relationship of immaterial labour in the context of machinic production. In "Machine Fragments" he states "The workers operating the apparatuses are just as much a part of the machine as the intellectual, cognitive labour of those who have developed the machine and make up its social environment" (22-23). Here the human has become an automaton, not simply as the meaty apparatus of a clunky mechanism, but as a real, objectified investment of human knowledge in the machine itself. The intellectual power of those people who conceptualised, designed, and produced the machine are invested in the machine in the ossified form of the general intellect. In this sense, all machines and tools are expressions of the individual intent that designed and constructed them, and have taken on a life of their own. As Marx states, they are "organs of the human brain, created by the human hand; the power of knowledge, objectified. [...] to what degree, hence, the conditions of the process of social life itself have come under the control of the general intellect and been transformed in accordance with it" (706). This 'general intellect' is one of the primary problematics that motivates arguments over the labour theory of value that have emerged recently around the issue of immaterial labour (for example, the dialogue between Fuchs, and Arvidson and Colleoni).

In their role as the conscious linkages between machines, humans are explicitly described as machinelike by Marx, because, in terms of their effects on the machinic systems of both the means and mode of production, a human being is the moving power which moves itself, but totally subject to the imposition of the conditions of their labour and to the mode of production - in other words, "an automaton" (692).

THE BASICS OF DDOS ATTACKS

The Distributed Denial of Service or DDoS attack is a methodology for functionally removing a node from a network. Yuan and Mills define a DDoS attack as "a simultaneous network attack on a victim (e.g., a Web server or a router) from a large number of compromised hosts, which may be distributed widely among different, independent networks. By exploiting asymmetry between network-wide resources and local capacities of a victim, a DDoS attack can build up an intended congestion very quickly at an attacked target" (2005, 324). The end-to-end structure, first argued for by Saltzer, et al., as the most efficient and effective means of structuring a computerised network, has since become the crux for a successful DDoS attack. A large number of attackers sending information to a victim computer, with the information framed either as requests for data, or as messages or instructions to be processed. These messages become a part of a process queue which has the capacity to deal with a limited amount of tasks. Once the queue is full, the system will not respond until it has finished processing at least some portion of the information - hence 'denial of service'. As long as an attack continues, the victim is unlikely to be able to process information at a sufficient rate in order to complete the queue, so the target may remain offline for as long as the attack continues. Large numbers of requests are necessary to fill process queues, and in order to achieve the necessary number of requests, the attack has to be come from a number of attack vectors - hence 'distributed'. With large numbers of attackers, and a small range of targets, the ratio of attack nodes to victims in an attack will tend to approximate a many-to-one relationship, which leads to the asymmetry in computing resources that Yuan and Mills refer to. Even if the target computer has a very high processing speed, it is difficult to deal with the sheer number of requests from the larger DDoS attacks. Because data packets are not generally acted upon between their source and destination,

other than to read addressing information, DDoS attacks are difficult to detect and prevent at locations other than at their target.

Despite that, DDoS attacks are not fool proof, and are able to be defended against. As Yuan and Mills point out, it is necessary to first detect the existence of an attack before a defence can be mounted. Because the nature of DDoS attacks involves great volumes of traffic, congestion occurs across the whole of the network, so to some extent the best defences occur upstream of the victim node. This is not always possible, as it requires coordination between the victim and their service provider, so it is necessary to have local measures that can deployed once a DDoS attack has begun. While a common enough response is for a victim to switch their operations to another more secure server, this is not always possible, particularly for small operations. In almost every other case, the defence protocols involve suspending or refusing connections with other nodes on the network, either by ignoring particular compromised servers, or certain ranges of IP addresses. By electing to refuse certain IP address ranges, this effectively still results in the server being removed from the network - a type of voluntary, rather than enforced exit. Modifying network settings to ignore particular IP ranges will still result in non-attacking IP addresses from being excluded. Even then, any attack program other than the most basic DDoS implementations will generally provide IP spoofing and other techniques for subverting defence mechanisms. Security firms and academic researchers are regularly involved in producing new techniques for defending against DDoS attacks. These are, at least somewhat, a proprietary service. At this stage, the DDoS attack remains a somewhat effective means of mobilisng a large number of computers towards various types of political dissent, although the outcomes of the specific DDoS attacks themselves still leave a lot to be desired in terms of political relevance.

The DDoS attack has many differing effects on the victim - for instance, increasing the costs in telecommunications charges, removing an institution's ability to communicate over networks, shutting out clients for businesses, disrupting financial transactions, loss of trades for commercial organisations, and so on. In political terms, it can show the vulnerability of corporations and nation states to the power of various collective practices. At times it can lead to the automated reset of servers, which opens the server to various security vulnerabilities for breaches by 'genuine' hackers. At the same time, corporations and nation states are more than capable of deploying large resources to disrupt the communications of individuals or political groups. Garnaeva and Namestnikov have an extensive analysis of DDoS attacks in 2011, and note that servers for the Israeli Defence Force, the Mossad, the Oakland police department, Mastercard, and Hong Kong Stock Exchange were high-profile targets of denial of service attacks.

In the context of a network operating on computerised network protocols, the DDoS attack methodology bases itself on the principle that a large number of attackers can consume the information processing resources at a target IP address. Because these targets are either individual servers or server clusters, whose function is dedicated to dealing with incoming requests, the attack needs to be coordinated to some extent. The DDoS attack is unique among network attack methodologies because, rather than requiring a vast amount of technical competency with the minutae of computer network protocols, operating system vulnerabilities, or other activities described as hacking or cracking, the DDoS attack works through simple brute force. This means that, at times, it is the result of actual democratic usage of the structure of the network in a manner that attacks the structure itself. From a Marxist perspective, that is a periodic and temporary mechanism for causing the machine of network capitalism to operate in its own terms against itself. A highly specific and short-lived self-destruction from which the system will eventually recover.

Because of these considerations, the DDoS attack methodology has the appearance of a form of post-political democratic protest - however it is precisely this appearance that this article seeks to undermine. The fact that the machines are used to engage in dissent in a representational form means that the DDoS attack methodology tends towards a non-democratic form - one could even say republican form, in the sense that certain well-connected individuals possess a disproportionate percentage of representative power. The reason that the system is not inherently democratic is because one user may mobilise multiple computers in the DDoS attack, and may automate this procedure over the network.

When the DDoS attack methodology is democratic is in its ability to allow self-representative dissent to occur over a network. That is, when one individual activates one computer as part of a political protest based on an effusion of presence. This has led various communities of dissent to refer to such acts as forms of 'digital sit-ins', a move that resurrects the political rhetorics of the civil rights movement. Such an analogy is duplicitous, as the purposes are different - the lunch counter sit-ins during the civil rights movement were geared towards allowing persons of non-European descent to be treated as equal consumers, with equal access to the space of the cafeteria. For 'digital sit-ins' the spaces are already fully accessible by all, and it is only with the disruption of the DDoS attack itself that access begins to be disrupted. Furthermore, the analogy has similarities to the idea of 'cyberspace' - an idea with little theoretical purchase. The target of the DDoS attack is a machine, not a space, and as such, the sit-in should be reconsidered as sabotage.

Here the DDoS attack acts as a new take on the old processes of sabotage. Rather than throwing one's shoes into the machinery, the political DDoS attack takes the form of an aggressive amount of attention to shut down the means of communication and subjectification. In the space of network communications in postindustrial capitalism, for sites that are totally dependent on the mechanisms of networks for their existence, this can be a substantial threat to continued operations. Sites such as eBay and Amazon, or transaction sites like PayPal and Mastercard could face serious financial consequences if their businesses were disrupted for even a short amount of time.

There are two ways to organise a DDoS attack - the first is social, the second is technical. In the social case, the sole requirement is that enough individuals are induced into making data requests simultaneously. This is something that can happen accidentally. For instance, the computer tech website Slashdot is a news-based link forum that holds many millions of members. When a link is posted to Slashdot by an editor, many hundreds of thousands of individuals often try to visit the site. When the hosting server is assigned only a moderate amount of data capacity, or data bandwidth, such as a hobby site, a small university or business, or similar, then the website can be shunted off the internet fairly quickly. This is called being "slashdotted". Various other large sites have equivalent names, but the mechanism is usually the same. The result is an unintentional DDoS attack. Because this is not a deliberate attack, the site will usually only be offline for a matter of hours. In comparison to deliberate technological DDoS attacks, Garnaeva and Namestnikov point to the longest intentional attack of late-2011 within their data as lasting over 80 days. In terms of organisational techniques, the social method of engaging in a DDoS attack by Anonymous is mobilised through short lived operational briefings, called "ops".

The technical method for engaging in a DDoS attack usually involves two things: a command and control, or C+C, server, and a set of compromised machines. Compromised machines are computers connected to the network that have been infected with some form of malware. By virtue of this malware, an external source can give instructions to the computer, most likely outside the knowledge of the computer's owner or users. C+C servers op-

erate to control vast numbers of compromised machines by acting as a host or source for instructions. Individual compromised machines are referred to as 'bots' and the network that is controlled by the C+C server is referred to as a 'botnet'. While a botnet can be deployed for any number of computational tasks - password cracking, spamming, deploying further viruses, and so on - our interest is in its role in DDoS attacks. It is also worth noting that botnets do not strictly require a C+C server for functionality, and control of the botnet can be achieved by means such as P2P network protocols; however, for our purposes this is functionally equivalent to the centralised form of control offered by a C+C server. The botnet receives instructions for attack vectors from the C+C server, and operates to attack their chosen targets. The processing power of a botnet can be massive: in 2010 Weaver estimated that the Conficker-C botnet, named after its infection malware, had over ten million compromised machines involved in its network. The potential power of such a network is sufficient to overpower many target computers several times over, which leads to the interesting case where botnets can, at times, be rented from their owners for the purposes of brute force password cracking, DDoS attacks, and other similar tasks.

For a sustained political use of the DDoS attack, it is necessary to find a mix of automated code and social engagement. Software is required to sustain a DDoS attack for longer than a few hours, so that the data requests that render an IP address unusuable remain consistent over time. The element of social engagement means that the quantity of invested individuals is increased to the point where the number of requests is sufficient to have an impact at the target computer.

One of the main parties that utilises DDoS attacks politically is the loose collection of individuals known as 'Anonymous'. Anonymous is a group that does its best to completely avoid any form of identity politics, and members usually make reference to themselves as 'anons' or in the third person as 'Anonymous'. Part of their slogan explicitly defines themselves as such: "We are Anonymous. We are Legion." Anonymous is mainly known as a decentralised online activist community with a strong free speech stance and a dislike of intellectual property laws, and a secondary position of anti-identity politics. While there are tensions between their dislike of "hate speech" and their advocacy of free speech, their general political position is roughly a form of anarchistic liberalism. Politically, Anonymous lacks a central tenet or principles for political activism, although there are many ad hoc social practices that fade in and out of relevancy. Although its inception was as an anti-Scientology collective, this later expanded to include attacks on the Westboro Baptist Church, before contributing to the Occupy Wall Street movement in 2011. Along the way, they have targeted organisations such as PayPal and Amazon, cyber-bullies and child pornography rings. Organised solely over networked communications, Anonymous generally engages in three forms of political activism: online and offline demonstrations, defacement or intrusion server hacks, and a presence in news media and social networking. Anonymous' members are diffuse, in the sense that individuals can join and leave at any time, and the success of any individual political action is roughly proportional to the number of members who subscribe to the political principles of the action. The individual political goals of members vary, and if the rhetoric that is deployed amongst their users is to be believed, they include all ranges of political position, including anarchistic, radically neoliberal, and communistic perspectives.

Anonymous' collectivity claims to be so broad as to include any and all individuals that are willing to become a part of it, or so they claim. The extent to which they attempt to achieve this is found in the "#OpNewBlood" project. This "operation" is a document that contains all the seed information for any individual with an internet connection to begin to communicate within the channels utilised by the Anonymous group. They have several

open access documents - released without any form of copyright license - that are designed to aid newcomers to their group. For instance, the "#OpNewblood Super Secret Security Handbook" details a number of techniques and basic information about HTML-based browsing security, Virtual Private Networks, and the use of virtual machines. The document "OpNewblood Guide for IRC Chat Setup & Anonymous Internet Browsing" provides basic information about joining Internet Relay Chat, or IRC, discussion groups. Tellingly, with regards to their open and free relationship to membership, their document ends with a reversal of their slogan: "Welcome. You are now Anonymous, but you were already. We are legion. Do not forgive. Do not forget. We were expecting you."

While there is a fair amount of internal political activity going on, in the sense of extensive IRC discussions on all manner of concerns, the main connection between Anonymous and the outside world is in terms of their disruption of computer networks. While often described as a 'hacktivist' group, the term is problematic and many of its members lack a great deal of prowess when it comes to actually engaging in sophisticated intrusion techniques. To this end, the group utilises a software application known as the Low Orbit Ion Cannon, or LOIC, to aid its less technologically advanced users in their protests. The application has a number of versions, usually recognisable due to their similarity in naming conventions: HOIC, JSLOIC, GOIC, LOIC2, and so on. The variations between each version are less important for this article, as the interface remains roughly the same between variations. When deployed by a user, the LOIC requires simply that a few details be inputted with regards to target IP addresses, frequency of attack, and a status window that declares the relative level of 'success' of the attack. While attacking, the application either sends simple messages or makes requests for data from the server. Each individual user contributes only a small amount to the greater portion of the DDoS attack, and a large number of individuals are required to contribute before the attack reaches the point where it effectively achieves anything. It is only when the number requests exceeds the rate at which the server can cope with the requests that the server is effectively pushed off the internet.

A technical analysis by Mansfield-Devine examines the nature of the LOIC application and its derivatives. Mansfield-Devine notes that most variants of the application lack any form of user protections, in the form of IP spoofing or other methods for hiding data about the LOIC's users. Pras (8) also notes that the instruction guide to the LOIC application distributed by Anonymous includes specific claims that the users of the tool will have a degree of protection that simply is not present. In fact, Pras et al note that one of the few protections that the users of the LOIC might have is the limits of legal jurisdiction to prosecute internationally.

To some extent, Anonymous' DDoS attacks are centrally orchestrated - some versions of the LOIC allow users to simply follow the 'hivemind' and follow attack instructions from specialised IRC threads. For the most part, individual involvement is spurious, and many attack attempts do not have sufficient levels of members involved to sustain successful attacks. Despite this, Anonymous continues to utilise DDoS attacks in political protests, and will likely continue to for the foreseeable future.

The Automaton

The purpose of using the idea of the automaton as an interrogative device is twofold. It conjures both the idea of a metastable machinic subjectivity that is distinct from - almost opposite to - the idea of the cyborg that dominates science fiction metaphors of post-industrial capitalism, and, also, as a product of this particular form of subjectivity, it fixes a particular relationship between the worker and the mode of production. Broadly, an

automaton is a form of machine, digital or otherwise, that generates an appearance of autonomy from any external control. At times this is the result of a sophisticated series of mechanisms - digital codes, hydraulic devices, moving weights, or clockwork gears - at other times it is the result of subterfuge. Numerous automata have existed where the device is not controlled by an internal series of mechanisms, but rather are powered by an individual hidden inside the machine; indeed all automata require an external motivator because no mechanism within the universe, whether mechanical, biological, or physical, is a totally self-contained system. Rather than state that these are somehow invalid or illegitimate automata, I would instead suggest that this is a central element to the concept of the automaton - the simulation of a machine subjectivity whose exact nature we cannot necessarily interrogate. In a computerised format, I would point to assemblages such as the artificial intelligence Cleverbot, as comparative examples of this phenomenon. Cleverbot is a chatterbot program that is designed to mimic human conversation; however, its database of conversations is not programmed into it. Instead, when a user interacts with it, it responds on the basis of the conversation habits of individuals it has communicated with previously. There is a machine in play, but it is only mobilised by the actions and behaviours of those that have come before, and any semblance of a subject emerging from the machine is only a product of these structures.

The etymology of *automaton* itself stretches back to antiquity, with its etymon emerging in ancient Greece. An automaton was a type of marionette, for the theatre or entertainment. In this role, the marionette was one whose operator was hidden or obscured from the view of the audience. In terms of its components, 'auto-' refers to the self, while '-maton' is cognate with 'mind'. The automaton is a type of synthetic entity that appears to act and move unbidden by external forces. The key, here, is 'appears': the source or cause of the automaton's movements is not immediately clear to the observer. Where the marionette was controlled by a puppeteer's strings, automatons were eventually developed to became internally controlled, whether by a series of complex clockwork gears powered by wound springs, or hydraulic systems that produced responses on the basis of ratios of water pressure.

The first independently mechanical devices to be called automatons were the devices of the first century inventor, Hero of Alexandria. These were simply, as Stafford and Terpak describe them, "early examples of complex machines" which held no resemblance to a human (266). But to those unfamiliar with the ideas of early science, they implied an unseen operator controlling the individual elements of machines. The idea of the automaton received new life in the 17th century, with the emergence of simple mechanisms added to the magnificent clocks of European cathedrals. Tom Standage writes, in *The Mechanical Turk*, that "these clocks often had astronomical features (such as the phase of the moon) and in some cases entire mechanical theatres that sprang to life on particular occasions" (3). Over time, these accoutrements became an attraction in their own right, and clock-making techniques were modified to produce wind-up mechanisms that operated on the basis of elastic energy potentials contained in spring systems inside the toy. These new developments became the basis for a thriving economy of jewel-encrusted devices that Britain exported in great quantities. When the eventual glut in the market arrived in the latter portion of the eighteenth century, museums opened in London to display all manner of automated "elephants, griffins, and obelisks" cast with opals, ivory and gold, along with other articles in a cabinet of curiosities that was open to the public (Stafford and Terpak, 269).

In the more modern appearances, an automaton is no longer simply any machine, but is instead a mechanical being that often simulates life. At times this simulation is a simple act of aesthetic representation; for instance, the 15th Century statue, known as the

Rood of Grace, was a crucifix that had a mechanical Jesus that could be controlled into turning its head, smiling, and giving the appearance of crying - but nothing more. In other cases automata involved a more sophisticated arrangement of mechanics or computer code to develop a behavioural semblance of a living being, or perform more pragmatic tasks. This includes a handwriting machine programmed by spindles, developed by Friedrich von Knauss, who is credited with being the inventor of the typewriter. Automata have increasingly, over history of the seventeenth, eighteenth, and nineteenth centuries, increased in their diversity of form. Records exist of mechanical eagles and lions, a brass fly, a jewel encrusted elephant, dancing ballerinas, harp-players, winged angels and more (Standage 3-5).

While being a consciously man-made mechanical device, whatever limited functional purposes the automaton is set to, some effort is made in its production to morphologically resemble a biological being. At times this meant that some automata were designed or built with rudimentary organs. Standage refers to Jacques de Vaucanson as designing three automata that had some semblance of internal organs: an automaton of a young boy that had functioning bellows that would allow it to play a flute, a second flute-player that also played a drum, and finally, a feathered metal duck that could eat grain and digest it in a rubber alimentary system (8-9).

Some models of automata took this idea of the emulation of a conscious being somewhat further. The famous Mechanical Turk that Standage has named his book after, is an interesting case in point. The Mechanical Turk was an automaton that was designed to play chess against a human opponent. Built in 1770 by Wolfgang von Kempelen, the machine featured a turbaned mannequin seated above a large wooden box filled with gears and cabling. By way of a mechanical hand, the 'Turk' would move pieces across the chessboard. The idea of a robot made from simple springs and cogs being as successful at chess is perhaps too fantastic to believe, especially when, for decades, supercomputers, such as Deep Blue, were required to play successfully against the top ranked human players. Indeed, the idea is too fantastic - the machine was designed such that it could accommodate a human player within the contraption, and gave them access to a control for the mechanical arm. Von Kempelen's deceit was not unusual amongst automata - Standage notes at least one other instance where a harp-playing automaton was found to contain a 5-year old child.

The Turk has since re-emerged as an un-ironic metaphor for the outsourcing of labour from machines to humans in Amazon.com's Mechanical Turk marketplace. Those using the Mechanical Turk marketplace are directly renting the computation power of human beings by passing large amounts of problems from a dataset into the Turk. Ten percent of the wage paid by the purchaser is passed on to Amazon, with the remaining portion going to the labourer. In this case the automaton houses not one, but thousands of human subjects. The purpose for this process is not simply to an imposed alienation of the labourer from the capitalist: certain organisational or mathematical problems are particularly difficult for a computer to resolve, and are best resolved by human operators - such as identifying images or the transcription of audio recordings. This has led to many interesting uses of the Mechanical Turk marketplace, although one in particular acts as a modern curiosity: Matt Richardson's 'Descriptive Camera' art project. The mechanics of the descriptive camera include a webcam, a thermal printer, and a network connection to Amazon's Mechanical Turk, combined into one apparatus. The project involves the camera sending photographs to the Turk with an instruction for human operators to textually describe the scene, and the description is sent back to the camera, which then prints the statement on the thermal printer.

A primary concern of early observers of these automata was the 'truth' of the mech-

anism - that is, whether the automaton held an unseen individual, or was truly a man-made simulacra of a living being. This concern is one that has become unnecessary or uninformative in the context of network communications. Alan Turing famously proposed an imitation game wherein an artificial intelligence emulates human qualities in order to convince a human player that they are talking with a flesh-and-blood being (1950, 433-436). Turing's game has spawned a variety of attempts to produce machinic subjectivities that have remarkably high 'pass rates' of convincing players that they are talking to a human being. Indeed, the authors of Cleverbot claim to have achieved a 59.3% 'humanity score' in a test against human players, where the human players only achieved a score of 63.3%. Notably, the judging committee has decreed score of over 50% is distinguished as 'human'. This does not mean that it is worthless to attempt to discern whether a subjectivity on the internet is human or otherwise, simply that the process of interrogation is rarely necessary for regular interaction, or for academic social theory. Artificial intelligences themselves are, after all, programmed by an author, and to this end are simply another layer of machinery between an author and an audience. Along this line, we can see the cohesion between the idea of the human being and the automaton, and can expand on this via a short examination of Descartes.

As early as 1630, Descartes argued that animals and other biological phenomena were nothing more than complex automata. According to Descartes, these *bÃªte machines* - 'beast machines' - were the product of God's mechanistic capabilities that would go unmatched by human beings (Cottingham, 551). This was not to deny that animals felt nothing, or that their pain was somehow illegitimate, but rather that they lacked what would be defined in contemporary contexts as a subjectivity or psyche. The nature of an automaton was nothing less than an understanding of all biological beings in the light of a Cartesean mechanistic understanding of the universe. Descartes' use of the term 'automaton' operates to define much of the modern understanding of automatons as synthetic and mechanical but also capable of generating affects in observers through their representations of alterity. Descartes believed that, although these automata were beyond the capacity of humans to create at the time did not mean that they were any less an automaton than one made of mechanical parts. What distinguished the human being from all other biological automaton was the presence of a divinely created soul, tied to the body through the pineal gland, and acts as the basis for a form of theological humanism. Descartes would later expand on this when he states:

"The key point to grasp, to my mind, is that no motions can take place, whether in animals' bodies or ours, unless these bodies contain absolutely all the organs or instruments by means of which the same motions could also be produced in a machine. So true is this, that not even in ourselves does the mind move the external limbs directly: it only directs the animal spirits that flow from the heart through the brain into the muscles, and determines them to specific movements, since of themselves the spirits are applied with equal facility to many different actions." (Descartes, 2008, 147) This is one perspective into Descartes' mind-body dualism, where subjectivity and psyche originate outside of the body, leaving the machinic automaton of the meaty body to act according to the whims of the spirit. Spirit, according to Descartes, is a quality that can only be held by human beings, whereas animals are left to an uncritical stimulus response with their environment. The presumption that humans and animals were both mechanical beings, but were somehow fundamentally different by virtue of a psyche exterior to the body, is something that the philosopher Eugene Thacker refers to as the "notorious analogy" (2010, 25). This, for Thacker, is emblematic of the notion of "superlative life" - where the category that defines what life is, is somehow external to the bodies in which life is expressed. This causes a split Superlative life seeks to be life as "generosity, as proliferation, as excess" and points to ideas of spirits and souls that are

external to social spaces (28). Superlative life is a transcendent idea of life that exceeds the system of the social world, and is difficult to utilise effectively in discussions regarding communication and subjectivity. Descartes' idea of the automaton pushes the individual subjects beyond the more material social concerns of networked political communication that I wish to examine.

Descartes' work has rhetorical and conceptual similarities to the position I am seeking to discuss, insofar as the subject's existence in the world is machine-like, but Descartes moves to transcend the subject/psyche to a position superior to the body in a manner that is difficult to utilise. Following Hayles' writing in the context of cyborgean humans, we should "turn Descartes upside down", and note that "conscious thought becomes an epiphenomenon corresponding to the phenomenal base the body provides" (1999, 203). Perhaps Deleuze and Guattari can enlighten us, with their quote from Lewis Mumford: "If a machine can be defined more or less in accord with the classic definition of Reuleaux, as a combination of resistant parts, each specialised in function, operating under human control to transmit motion and to perform work, then the human machine was a real machine" (1987, 504-505). My approach, unlike Descartes, wishes to be totally immanent to the world of networks, and in order to do this, we will turn to the works of Karl Marx.

Marx shows the automaton as a framing device for political subjectivities in networks in the pages of the Grundrisse, where humans have been reduced to the meaty parts of machine networks. There is an alternative, but compatible, position in the works of Deleuze and Guattari - particularly developed in Guattari's works in the early 1980s - and a contemporary framing in the work of Gerald Raunig, that deals with the expansion of these network ideas from a purely mechanical network, into a social use of the idea of the automaton. These four thinkers develop the idea of the automaton, not as a *larvatus prodeo* subjectivity of the ghost in the machine, but instead as a totally immanent machine within the machine.

Before continuing onto the discussion of networks, it is worth discussing the limitations of the idea of the automaton. To use the automaton as a figure of the post-industrial subject of capital in this manner is to reduce the individual conditions of work to the lowest common denominator, and - in the context of an immanent approach - limits the notion of agency by almost removing it entirely. Doing this rides roughshod over the differences in the conditions of labour within post-industrial capital - that is, the concept of the automaton can conveniently apply itself to industrial and agricultural labour, and primarily ignores affective forms of labour, it does so at the cost of analytical scrutiny of these important issues.

These drawbacks are opposed to the strength that is finding a means of discussing labouring subjects within social machines in terms of a common grounding that allows us to examine collectivities without subsuming individuation any further. This means that the issue of identity politics is removed from the equation. Identity politics is a difficult beast to deal with in online spaces, in the sense that the technologies of communication obliterate physiological distinctions between individuals. Once these distinctions begin to disappear, there is no strong categorical system for defining individuals communicating over a network. 'Disappear' is used advisedly here: the disappearance does not equate to an end to the politics of identity, but rather a terrain that poses problems of visibility for identity. This is the issue that Turing's imitation game brings to the fore - we are always less than one hundred percent certain of who we are communicating with over the internet. Once categories based around identity have been disappeared, various forms of patterns can be seen to emerge that are temporary and shifting that are otherwise interpreted as elements occurring within a particular form of politics, when, instead, they are open and unconstrained by

rigid boundaries of particular forms of physiological identity.

RECONCILITATION

So then, to what end does an informal, open, and vulnerable group like Anonymous,and the crude means by which it engages in DDoS attacks have any use for an analysis through the automata? In order to understand this, it is first necessary to understand that the open and collaborative organisation of the political actions that Anonymous takes part in appears to be a ruse, and that probably many members are unaware of this fact. As Mansfield-Devine notes, the ability for members of Anonymous to communicate effectively within such an anarchic structure is all well and good, but majority of the most successful attacks seem to be organised outside of the input of the community itself. When an attack bulletin is released, many members will simply accede to the instructions. Because these bulletins are often released or redistributed 'in the wild', the only quality that officiates them is a particular aesthetic approach - this has led to the Westboro Baptist Church covertly releasing attack documents in the same style as Anonymous' regular releases, ostensibly in order to obtain attackers' IP addresses for purposes of litigation (see "Message to the Westboro Baptist Church, the Media, and Anonymous as a Whole."). In the gap between the discussions that occur within the Anonymous communication channels, and the actual attack instructions, there is a space for manipulation, and Mansfield-Devine suggests that this is a space that is employed by the organisational core to Anonymous, which effectively manipulates the community's desire for action into specific tasks. Some of these individuals have already been arrested since Mansfield-Devine's publication. Eighteen year old Jake 'Topiary' Davis was famously arrested at his home on the extremely isolated Shetland Islands for running multiple Twitter accounts for a group closely associated with Anonymous, while Hector 'Sabu' Monsegur turned as a informant for the group after being arrested for hacking by the FBI. Sixteen people were arrested mid-2011 for their alleged involvement with Anonymous and - contrary to popular expectations that they would be all teenagers, their median age was 24 (Winter, 2011). Mansfield-Devine's assessment of a central organisational core to Anonymous suggests that the majority of the members are simply part of an ablative attack vector for a central command that designates the actions of the group.

To this extent, if we speak with an analysis that addresses the functionality of the social machine of Anonymous, rather than as a conspiracy, then Anonymous operates to draw in large numbers of politically committed individuals who have little capacity to identify other individuals within the group. Furthermore, they will operate in terms of the instructions given out through the organisational documents, simply pointing their LOIC applications at the appointed target, and clicking the proper button. When the political dissent is so systematised, controlling a large number of compromised computers in a botnet is not altogether different from organising a large number of individuals to accomplish the same task. The functional difference between a C+C server that mobilises a compromised computer to make spurious data requests of a target, and an online manifesto that mobilises an individual to do the same, is very small when it comes to the victim.

Given that, under these conditions, the individual members of Anonymous are largely unimportant and undifferentiated, they have no strict identity of their own beyond the few traces that they leave on the network, their political influence on the network is largely a product of already-defined manifesto materials, and their subject presence outside of the network is not connected to the mechanisms of their online presence, then they are an excellent example of the automation of political dissent.

A DDoS attack by Anonymous is not the only political action that can be addressed

through this paradigm of the machine/automaton, nor should it simply be used to analyse democratic or capillary instances of dissent. As Goncharov reports, in Russia in late 2011, anti-Putin political protests were being organised over Twitter under a particular set of hashtags. These hashtags, and others like them, were soon rendered unusable as pro-government activists mobilised bot accounts to post to these hashtags at a rate of up to 10 posts per second. Twitter quickly became unusable for political organisation of democratic protest. Here the machine of political oppression exploited the mechanisms of dissent to its own ends.

The extent to which a paradigm of automated dissent ceases to be useful is exactly the same point where political dissent stops being mobilised over technological machines. For the remaining cases of digital activism, the paradigm is informative when it comes to analysing the production of particular forms of subjectivity in the context of network politics that attempt to exist outside of other forms of politics.

References

"Amazon Mechanical Turk." Web. 8 Aug. 2012.

Arvidsson, Adam, and Eleanor Colleoni. "Value in Informational Capitalism and on the Internet." *The Information Society* 28.3 (2012): 135-150. Print.

Carpenter, Rollo. "Cleverbot.com." Web. 31 July 2012.

Coleman, Gabriella. "Our Weirdness Is Free." *Triple Canopy* 15 (2012): n. pag. Web. 27 Nov. 2012.

Cottingham, John. "'A Brute to the Brutes?': Descartes' Treatment of Animals." *Philosophy* 53.206 (1978): 551-559. Print.

Deleuze, Gilles, and Felix Guattari. *A Thousand Plateaus: Capitalism and Schizophrenia*. Vol. 2. Continuum International Publishing Group, 2007. Print.

Descartes, R. *Meditations on First Philosophy: With Selections from the Objections and Replies*. Trans. M. Moriarty. Oxford University Press, USA, 2008. Print.

Engels, Frederick. "The Mining Proletariat." *Condition of the Working Class in England*. 1845. Web. 6 Aug. 2012.

Fuchs, Christian. "Labor in Informational Capitalism and on the Internet." *The Information Society* 26.3 (2010): 179-196. Print.

---. "With or Without Marx? With or Without Capitalism? A Rejoinder to Adam Arvidsson and Eleanor Colleoni." *tripleC* 10.2 (2012): 633-645. Print.

Garnaeva, Maria, and Yury Namestnikov. "DDoS Attacks in H2 2011." *Kaspersky Securelist*. Web. 8 Aug. 2012.

Goncharov, Maxim. "The Dark Side of Social Media." *TrendMicro Malware Blog*. Web. 13 Aug. 2012.

Guattari, Felix, and Antonio Negri. *Communists Like Us: New Spaces of Liberty, New Lines of Alliance*. Semiotext (e) New York, 1990. Web. 8 Aug. 2012.

Hardt, Michael, and Antonio Negri. *Empire*. 1st ed. Cambridge, Massachusetts: Harvard University Press, 2000. Print.

Hayles, N. K. *How We Became Posthuman*. University of Chicago Press Chicago and London, 1999. Print.

Mansfield-Devine, Steve. "Anonymous: Serious Threat or Mere Annoyance?" *Network Security* 2011.1 (2011): 4-10. Print.

Marx, Karl. *Grundrisse*. Trans. Martin Nicolaus. Penguin Books, 1973. Print.

"Message to the Westboro Baptist Church, the Media, and Anonymous as a Whole." *Anonnews.org*. Web. 9 Aug. 2012.

Murphy, Timothy S. *Antonio Negri: Modernity and the Multitude*. Polity, 2012. Print. Key Contemporary Thinkers.

"OpNewblood Guide for IRC Chat Setup & Anonymous Interneting." *CyberGuerrilla AnoNneXus*. Web. 9 Aug. 2012.
Pras, A. et al. "Attacks by 'Anonymous' WikiLeaks Proponents Not Anonymous." (2010): n. pag. Web. 9 Aug. 2012.
Raunig, G. *A Thousand Machines*. Trans. Aileen Derieg. Cambridge, Massachusetts: Semiotext(e), 2010. Print. Intervention Series 5.
Richardson, Matt. "Descriptive Camera." Web. 31 July 2012.
Riskin, Jessica. "Machines in the Garden." *Republics of Letters* 1.2 (2010): 16-43. Print.
Saltzer, J. H., D. P. Reed, and D. D. Clark. "End-to-end Arguments in System Design." *ACM Transactions on Computer Systems (TOCS)* 2.4 (1984): 277-288. Print.
Sandry, Eleanor. "Dancing Around the Subject with Robots: Ethical Communication as a 'Triple Audiovisual Reality'." *PLATFORM: Journal of Media and Communication* 4.1 (2012): 79-90. Print.
Shakarian, Paulo, and Damon Paulo. "Large Social Networks Can Be Targeted for Viral Marketing with Small Seed Sets." *arXiv:1205.4431* (2012): n. pag. Web. 9 Aug. 2012.
Stafford, B. M., F. Terpak, and I. Poggi. *Devices of Wonder: From the World in a Box to Images on a Screen*. Getty Publications, 2001. Web. 2 Aug. 2012.
Standage, Tom. *The Mechanical Turk*. Allen Lane The Penguin Press, 2002. Print.
Thacker, Eugene. *After Life*. Chicago and London: University of Chicago Press, 2010. Print.
"The #OpNewblood Super Secret Security Handbook." *pastehtml*. Web. 9 Aug. 2012.
Turing, Alan M. "Computing Machinery and Intelligence." *Mind* 59.236 (1950): 433-460. Print.
Weaver, R. "A Probabilistic Population Study of the Conficker-C Botnet." *Passive and Active Measurement*. 2010. 181-190. Web. 9 Aug. 2012.
Winter, Jana. "16 Suspected 'Anonymous' Hackers Arrested in Nationwide Sweep | Fox News." *FoxNews.com*. Web. 9 Aug. 2012.
Yuan, Jian, and Kevin Mills. "Monitoring the Macroscopic Effect of DDoS Flooding Attacks." *IEEE Transactions on Dependable and Secure Computing* 2.4 (2005): 324-335. Print.