Robert Jackson

FOUR NOTES TOWARDS PROPAGANDA AND THE POST-DIGITAL SYMPTOM

APRJA Volume 3, Issue 1, 2014
ISSN 2245-7755

> *This statement is still somewhat lacking in definiteness, and will remain so […] The statement is moreover one which one does not attempt to prove. Propaganda is more appropriate to it than proof, for its status is something between a theorem and a definition. In so far as we know a priori what is a puzzle and what is not, the statement is a theorem. In so far as we do not know what puzzles are, the statement is a definition which tells us something about what they are. (Turing, "Solvable and Unsolvable Problems", 588)*

This unassuming quote appears in, (what would be) Turing's final published article "Solvable and Unsolvable Problems" (1954). Out of context Turing's argument doesn't mean much, yet it is that word with stands out: propaganda. It is completely unrelated to any of Turing's other descriptions. What is it about propaganda that Turing deemed sufficient in describing a statement about puzzles, problems and solutions?

Despite not being an overtly political writer, Turing's relevancy is undoubtedly important for the politics of digital culture today: particularly concerning relationships between culture, computation, mathematics, digital transmission and even the purported recognition of the "post-digital". What on earth provoked him to describe a mathematical idea as propaganda? Might it not be understood as a retroactive sign of a post-digital affect, or, perhaps an expected symptom of embedded life within a politics of mathematical propagation? The purpose of these notes is to outline what such a description might provoke.

1. The efficacy of the digital

An obvious problem comes from the discourse of 'the digital' itself: a moniker which points towards units of Base-2 arbitrary configuration, impersonal architectures of code, massive extensions of modern communication and ruptures in post-modern identity. Terms are messy, and it has never been easy to establish a 'post' from something, when pre-discourse definitions continue to hang in the air. As Florian Cramer articulates so well, 'post-digital' is something of a loose, 'hedge your bets' term, denoting the general tendency of accounting for the digital revolution whilst acknowledging its innovations and political effects (Cramer).

Perhaps it might be aligned with what some have dubbed "solutionism" (Morozov) or "computationalism" (Berry 129; Golumbia 8): the former critiquing a Silicon Valley-led ideology oriented towards solving liberalised problems through efficient computerised means. The latter establishing the notion (and critique thereof) that the mind is inherently computable, and everything associated with it. In both cases, digital technology is no longer just a business for privatising information, but the business of extending efficient, innovative logic to all corners of society and human knowledge. Here then, the 'post-digital' logic might condemn every action through a cultural logic of efficiency and proprietary.

In fact, there is a good reason why 'digital' might as well be an synonym for 'efficiency'. Before any consideration is assigned to digital media objects (i.e. platforms, operating systems, networks), consider the inception of 'the digital' as such: that is *information theory*. If information was a loose, shabby, inefficient method of vagueness specific to various mediums of communication, Claude Shannon compressed all forms of

communication into a universal system with absolute mathematical precision (Shannon). Once transmission became digital, the conceptual leap of determined symbolic logic was set into motion, and with it, the 'digital' became synonymous with an ideology of effectivity. No longer would miscommunication be subject to human finitude, distance and time, but only the limits of entropy and the matter of automating messages through the support of alternating 'true' or 'false' relay systems.

However, it would be quite difficult to envisage any 'post-computational' break from such discourses — and with good reason: Shannon's breakthrough was only systematically effective through the logic of computation. So the old missed encounter goes: Shannon presupposed Turing's mathematical idea of computation to transmit digital information, and Turing presupposed Shannon's information theory to understand what his Universal Turing Machines were actually transmitting.

The basic theories of both have not changed. Instead, the necessary materials have provided greater processing power, extensive server infrastructure and larger storage, propagating Turing and Shannon's ideas beyond what they thought or expected. Some historians even speculate that Turing may have made the link between information and entropy two years before Bell Labs did (Good).

Thus this 'post-digital' logic of efficiency might historically acknowledge Shannon's digital efficiency, and Turing's logic. But by the same measure, any critical reflection on it must document how the logic of efficiency has transformed work, life, culture as well as artistic praxis and aesthetics. This is not to say that everything is reducibly predicated on efforts made in computer science. Instead one must fully acknowledge these dominant structures and account for how ideological principles operate within them, whilst restricting other alternatives which do not fit such a 'vision'. Hence, the 'post-digital' interpretation is as much a symptom of acknowledging this infrastructure, as it is, its own failure to address such implications. Perhaps the 'task' set for us nowadays might consist in critiquing digital efficiency and how it has come to work against commonality, despite transforming the majority of Western infrastructure in its wake.

Propaganda has some historical context here, and it exists in cryptography and concealment. It is well known that in 1943, Shannon and Turing had many lunches together, holding conversations and exchanging ideas, yet they never revealed detailed methods of cryptanalysis so integral to their lives (Price & Shannon). This provides us with a succinct allegorical image not only of their missed encounter, but also of their influential ideas: neither of which ever affords an ability to be transparent. Computational and digital transmission is never neutral, nor open, nor clear about what it does. Its automated decisions always conceal inherent principles of ideal forms that benefit those who construct them.

But in saying this, I do not just mean that the capitalist means of production *only* uses digital networks for propagative means (although that happens), but that the *very means of computing a real concrete function is constitutively propagative*. No system is ever 'neutral'. In this sense, propaganda resembles an understanding of what it means to be integrated into an ecology of efficiency, symptomatic of living 'post-digitally' or pretending to. Digital information often deceives us into accepting its objective, mathematical transparency, and of holding it to that account: yet in reality it does the complete opposite, with no given range of judgements available to detect manipulation from didactic lesson, nor persuasion from smear.

Thus the role of computation in digital networks affords a similar proposition. We all know that the 'web' is lying to us: it keeps telling us we are involved, or rather we have confused involvement with the 'fear of missing out'. Propaganda might be the practice of being always-already implicated with someone else's conceptual principles. Such principles embed pre-determined decisions which not only *generate* but *decide* on user choices and implicitly engage with them in the effort of solving a problem.

Propaganda obfuscates the means of transforming itself by its own use, such is the efficacy of propagating. It establishes itself by eschewing any systemic implication, thus becoming concealed behind other user attitudes. It denotes the verb to *propagate*: that is, to *reproduce ideas*, such is the inherent logic of ideology. Propagative logic is at its most potent in digital culture when machines operate silently, spreading and transforming ideas and decisions across global networks and functional systems.

Propagation operates in the logic of transmission: that of communication and control existing as one system, as Wiener's cybernetics knew so well. As Siegfried Zielinski recently noted in *[After the Media]: News from the Slow-Fading Twentieth Century* (2013), the discipline of cybernetics, so intimately related to Turing's work, is comparable to the study of propaganda. Quoting Zielinski, both disciplines share, "the intention of using applied mathematics to describe what is difficult to calculate or predict, and to monitor it in tests, which at the same extend the promise of controlling it". (Zielinski 25). The concrete practice of propagation is operative as soon as any transformed motion of binary signal is transmitted in a favourable direction through a medium, any medium. But more than the above, propaganda might be the inherent operation of solving all problems: most notably mathematical ones.

2. A decision problem

Two years before Shannon's famous Masters thesis, Turing published what would be his famous theoretical basis for computation in the 1936 paper "On Computable Numbers, with an Application to the Entscheidungsproblem." The focus of the paper was to establish the idea of computation within a formal system of logic, which when automated would solve particular mathematical problems put into function (Turing, *An Application*). What is not necessarily taken into account is the mathematical context to that idea: for the foundations of mathematics were already precarious, way before Turing outlined anything in 1936. Contra, the efficiency of the digital, there is a precariousness built-in to computation from its very inception: the precariousness of solving all problems in mathematics.

The key word of that paper, its key focus, was on the *Entscheidungsproblem*, or decision problem. Originating from David Hilbert's mathematical school of formalism, 'decision' means something more rigorous than the sorts of decisions in daily life. It really means a 'proof theory', or how analytic problems in number theory and geometry could be formalised, and thus efficiently solved by provable theorems (Hilbert 3). Solving a problem is simply finding a provable 'winning position' in a game. Similar to Shannon, 'decision' is what happens when an automated system of function is constructed in such a sufficiently complex way, that an algorithm can *always* 'decide' a binary, yes or no answer to a mathematical problem, in a sufficient amount of time given an arbitrary input. It does not require ingenuity, intuition or heuristic gambles, just a combination of simple consistent formal rules and a careful avoidance of contradiction.

The two key words there are 'always' and 'decide'. The progressive end-game of twentieth century mathematicians who, like Hilbert, sought after one simple totalising conceptual system to decide every mathematical problem and work towards absolute knowledge. All Turing had to do was make explicit Hilbert's implicit computational treatment of formal rules, manipulate symbol strings and automate them using an 'effective' or 'systematic method' (Turing, *Solvable and Unsolvable Problems* 584) encoded into a machine. This is what Turing's thesis meant (discovered independently to Alonzo Church's equivalent thesis (Church)): any systematic algorithm solved by a mathematical theorem in a proof, can be computed by a Turing machine (Turing, *An Application*), or in Robin Gandy's words, "[e]very effectively calculable function is a computable function" (Gandy).

Thus *effective procedures decide problems*, and they resolve puzzles providing winning positions (like theorems) in the game of functional rules and formal symbols. In Turing's words, "a systematic procedure is just a puzzle in which there is never more than one possible move in any of the positions which arise and in which some significance is attached to the final result" (Turing, *Solvable and Unsolvable Problems* 590). The significance, or the winning position, becomes the crux of the matter for that problem: *what puzzles or problems are to be decided and what solutions are afforded?* This is what formalism attempted to do: encode everything through the regime of formalised efficiency, so that all of mathematically inefficient problems are, in principle, ready to be solved. Programs are simply proofs: if it can be proved in discrete mathematics, it could be computed and automated.

In 1936, Turing showed how some complex mathematical concepts (or effective procedures) could simulate the functional decisions of all the other ones (such as the Universal Turing Machine). Ten years later, Turing and John von Neumann would independently show how physical general purpose computers, offered the same thing. From that moment on (broadly speaking), efficient digital decisions began to embed themselves in the cultural application of physical materials. Before Shannon's information theory offered the precision of transmitting information, Hilbert and Turing developed the structure of that transmission in the mathematical regime of formal decision.

Yet, there was also a non-computational importance here, for Turing was also fascinated by what decisions couldn't compute. His thesis was quite precise, so as to elucidate that if no mathematical problem could be proved, a computer was not of any use. In fact, the entire focus of his 1936 paper, often neglected by Silicon Valley cohorts, showed that Hilbert's particular decision problem *could not be solved*. Unlike Hilbert, Turing was not interested in using computation to solve every problem, but as a curious endeavour for surprising intuitive behaviour. The most important of all, Turing's halting, or printing problem was influential, precisely as it was *undecidable*; a decision problem which couldn't be decided, as no 'higher' algorithm existed to replicate the proof (what is commonly known as the halting problem).

Undecidable problems might be looked at as a dystopian counterpart against the utopian efficient solutions constitutive of Shannon's 'digital information' theory. A base 2 binary system of information transmission only works via the computational work of deciding on one of two possible states. Thereby a system can communicate with another via processing one digit, by virtue of the fact that there is only one other alternative digit to it. Yet any efficient transmission of that information, is only subject to a system which can '*decide*' on the digits in question,

and establish a formalised proof to calculate and modify the success of the transmission's direction. If there is no mathematical proof to decide a problem, then transmitting information becomes problematic for establishing a solution. Proofs, decisions and computation go hand in hand.

3. Decisional ecologies

What has become clear is that the post-digital world is no longer simply accountable to human decision alone. Decisions are no longer limited to the borders of human decisions and 'culture' is no longer simply guided by a collective whole of social human decisions. Nor is it reducible to one harmonious 'natural' collective decision which prompts and pre-empts everything else. Instead we seem to exist in an *ecology of decisions*: or better yet *decisional ecologies*. Before there was ever the networked protocol (Galloway), there was the computational decision. Decision ecologies are already set up before we enter the world, implicitly coterminous with our lives: explicitly determining a quantified or bureaucratic landscape upon which an individual has limited manoeuvrability.

Decisions are not just digital, they are continuous as computers can be: yet decisions are at their most efficient and effective when digitally transmitted. Decisional efficiency seeps into every neo-liberal treatment of engaging with a problem: forms, bureaucracy, quantification and administration. We are constantly told by governments and states that are they making 'tough' decisions in the face of austerity. CEOs and Directors make tough decisions for the future of their companies and 'great' leaders are revered for being 'great decisive leaders': not just making decisions quickly and effectively, but also settling issues and producing definite results.

Even the word 'decide', comes from the Latin origin of '*decidere*', which means to determine something and 'to cut off.' Algorithms in financial trading know not of value, but of decision: whether something is marked by profit or loss. Drones know not of human ambiguity, but can only decide between kill and ignore, cutting off anything in-between. Constructing a system which decides between one of two digital values, even repeatedly, means cutting off and excluding all other possible variables, leaving a final result at the end of the encoded message. Making a decision, or building a system to decide a particular ideal or judgement *must force other alternatives outside of it*. Decisions are always-already embedded into the framework of digital action, always already deciding what is to be done, how it can be done or what is threatening to be done. It would make little sense to suggest that these entities 'make decisions' or 'have decisions', it would be better to say that they *are decisions* and *ecologies are constitutively constructed by them*. Digital efficiency is simply about the expansion of automating decisions and what sort of formalised significances must be propagated in order to solve social and economic problems, which creates new problems in a vicious circle.

The question can no longer simply be 'who decides', but now, 'what decides?' Is it the cafe menu board, the dinner party etiquette, the NASDAQ share price, Google Pagerank, railway network delays, unmanned combat drones, the newspaper crossword, the javascript regular expression or the differential calculus?

One pertinent example: consider George Dantzig's *simplex algorithm*: this effective procedure (whose origins began in multidimensional geometry) can always decide solutions for large scale optimisation problems which continually affect multi-national corporations. The simplex algorithm's

proliferation and effectiveness has been critical since its first commercial application in 1952, when Abraham Charnes and William Cooper used it to decide how best to optimally blend four different petroleum products at the Gulf Oil Company (Elwes 35; Gass & Assad 79). Since then the simplex algorithm has had years of successful commercial use, deciding almost everything from bus timetables and work shift patterns to trade shares and Amazon warehouse configurations. According to the optimisation specialist Jacek Gondzio, the simplex algorithm runs at "tens, probably hundreds of thousands of calls every minute" (35), always deciding the most efficient method of extracting optimisation. The technique of decision might be a *propagative* method for embedding knowledge, optimisation and standardisation techniques in order to solve problems combined with the greater urge to solve the most unsolvable ones, including us.

Elsewhere Google do not build into their services an option to pay for the privilege of protecting one's privacy: the entire point of providing a free service which purports to improve the problems of daily life, is that it primarily benefits the interests of shareholders and extends commercial agendas. James Grimmelmann gave a heavily detailed exposition on Google's own 'net neutrality' algorithms and how biased they happen to be. In short, PageRank does not simply decide relevant results, it *decides visitor numbers* and he concluded on this note: "With disturbing frequency, though, websites are not users' friends. Sometimes they are, but often, the websites want visitors, and will be willing to do what it takes to grab them." (Grimmelmann 458)

Propaganda might not simply exist as biased representable information, but the very ecology of functional processes that effectively construct such a bias. Net neutrality assumes that technologies are never inherently propagative, but forgets that regimes of standardisation and formalisation, were already 'built in' to the theories which developed digital methods and means, irrespective of what computers can or cannot compute or prove.

The issue is what sort of significant result arises from these proofs, and what sort of principles are established in a given decision ecology: thus *mathematical algorithms are hard-wired ideological automatons*. As Plato knew, *an idea is an idea*, just as a decision only decides, regardless of its material basis.

4. Encryption and propaganda

But what of propaganda itself? What about the very idea of it? The familiarity of propaganda is manifestly evident in religious and political acts of ideological persuasion: brainwashing, war activity, political spin, mind control techniques, subliminal messages, political campaigns, cartoons, belief indoctrination, media bias, advertising or news reports. A definition of propaganda might follow from all of these examples: namely, the systematic social indoctrination of biased information that persuades the masses to take action on something which is neither beneficial to them, nor in their best interests. As Peter Kenez argues, propaganda is "the attempt to transmit social and political values in the hope of affecting people's thinking, emotions, and thereby behaviour" (Kenez 4) Following Stanley B. Cunningham's watered down definition, propaganda might also denote a helpful and pragmatic "shorthand statement about the *quality of information transmitted and received* in the twentieth century" (Cunningham 3), insofar as the twentieth century is sometimes referred to as the 'century of propaganda'.

But propaganda isn't as clear as this general definition makes out: in fact what makes propaganda studies such a provoking topic is that nearly all literature notes from the start, that no stable definition exists. Propaganda's definition is in itself deceptive. It moves beyond simple 'manipulation' and 'lies', unsubtle derogatory, jingoistic representations, and the irrational spread of emotional pleas, and extends to the ambiguity of constructing truth. As the master propagandist William J. Daugherty wrote:

> *It is a complete delusion to think of the brilliant propagandist as being a professional liar. The brilliant propagandist […] tells the truth, or that selection of the truth which is requisite for his purpose, and tells it in such a way that the recipient does not think that he is receiving any propaganda. (Daugherty 39).*

Propaganda, like ideology, works by being inherently implicit and social. In the same way that post-ideology apologists ignore their symptom, propaganda is keenly ignored in digital culture. It isn't to be taken as a shadowy fringe activity, blown apart by the democratising fairy-dust of 'the Internet'. As many others have noted, the purported 'decentralising' power of online networks, simply offers new methods for propagative techniques, or 'spinternet' strategies, evident in China amongst other regimes (Brady). Iran's recent investment into video game technology only makes sense, only when you discover that 70% of Iran's population are under 30 years of age, underscoring a suitable contemporary method of dissemination. Similarly in 2011, the New York City video game developer Kuma Games was mired in controversy when it was discovered that an alleged CIA agent, Amir Mirza Hekmati, had been recruited to make an episodic video game series intending to "change the public opinion's mindset in the Middle East." (Tehran Times). The game in question, *Kuma\War* (2006 – 2011) was a free-to-play First-Person Shooter series, delivered in episodic chunks, the format of which attempted to simulate biased re-enactments of real-life conflicts.

But propaganda is not just social, it is also tied up with understanding technical procedures and technique in general. Despite his unremarkable leanings towards Christian realism, Jacques Ellul famously updated propaganda's definition as the end product of what he previously lamented as 'technique'. Instead of viewing propaganda as a highly organised systematic strategy for extending the ideologues of peaceful warfare, he understood it as a general social phenomenon in contemporary society.

Ellul outlined two general types amongst other distinctions: *political* and *sociological* propaganda: Political propaganda involves governmental administrative techniques which intend to directly change the political beliefs of an intended audience. By contrast, sociological propaganda is the implicit unification of involuntary public behaviour which creates images, aesthetics, problems, stereotypes, the purpose of which aren't explicitly direct, nor overtly militaristic. Ellul argues that sociological propaganda exists; "in advertising, in the movies (commercial and non-political films), in technology in general, in education, in the *Reader's Digest*; and in social service, case work, and settlement houses" (Ellul 64). It is linked to what Ellul called "pre" or "sub-propaganda": that is, an imperceptible persuasion, silently operating within ones "style of life" or permissible attitude (63).

Faintly echoing Louis Althusser's Ideological State Apparatuses (Althusser 182) nearly ten years prior, Ellul defines pre-propaganda as "the penetration of an

ideology by means of its sociological context." (63) Sociological propaganda is inadequate for decisive action often meaning that the more repressive strategies of political propaganda are required. In the post-digital world, such implicitness no longer gathers wartime spirits, but instead propagates the social with proprietary principles: a neo-liberal way of life that is individualistic, wealth driven, cynical, proprietary and self-opinionated.

Ellul's most powerful assertion is that 'facts' and 'education' are part and parcel of the sociological propagative effect: nearly everyone faces a compelling need to be opinionated and we are all capable of judging for ourselves what decisions should be made, without at first considering the implicit landscape from which these judgements take place. One can only think of the implicit digital landscape of Twitter: the archetype for self-promotion, quip-formations and overly self-important methods of propagation — all taking place within Ellul's sub-propaganda of data collection and concealment. Such methods, he warns, will have "solved the problem of man" (xviii).

But the technique of information is of relevance here, and propaganda is only effective within a social community when it offers the means to solve problems by actively transmitting ideas in a particular direction: quoting Ellul:

> *Thus, information not only provides the basis for propaganda but gives propaganda the means to operate; for information actually generates the problems that propaganda exploits and for which it pretends to offer solutions. In fact, no propaganda can work until the moment when a set of facts has become a problem in the eyes of those who constitute public opinion (114).*

Looking at Ellul's quote sideways, the issue isn't that strategies have simply adopted contemporary technology to propagate an impressionable demographic, but that information is simply *always-already efficient, effective and propagative in its automation*. Thus for Ellul, "propaganda is called upon to solve problems created by technology, to play on maladjustments and to integrate the individual into a technological world" (Ellul xvii).

Let's return to Turing's quote, given from the outset. The statement he refers to as propaganda, is not immediately obvious to the reader, yet on closer inspection it actually refers to the Church-Turing thesis already mentioned. Might it not allude to this predetermined structures for how something can be effectively calculable? (Rosser): that Turing's own statement is not just capable of automating propaganda, *but just simply is propaganda*?

But why would Turing define a mathematical idea as *propaganda rather than proof*? He was well aware that his statement was *not an effective procedure in itself, which is to say the thesis itself cannot be proved* — it is certainly about proofs, or how one can prove certain things in a formal system (hence it might be a theorem) and what formal methods can automate them, but it *doesn't give us knowledge about what computational or systematic procedures are*. The statement only tells us that automated machines can decide the same winning conditions through equivalent algorithmic methods (its definition). The statement or thesis does not prove why computation might be able to solve problems at all — moreover it can't even tell us whether a problem can be solved, before one even attempts to find a solution (there is no effective procedure to 'decide' every effective procedure, as the halting problem suggests). Thus following Turing, there is no 'correct' use of applying

the thesis in practice: it resembles a theorem which seems to *propagate proofs*, yet, mathematically it only stands as a definition.

Formal systems certainly seem to offer effective procedures to problems, but unless a winning position is proved outright, it can never fully justify itself in offering solutions in all cases. *There is no effective procedure to guarantee a proof about what effective procedures are*, and this is what Turing might have meant: *there is no guaranteed calculation which calculates all other calculations*. There is only concrete instances of propagative functions that give us second-hand truths.

Turing's propaganda works much like Hilbert's progressive project of formalism, operating *as if* it can always decide solutions to problems, yet in its operation, must hide uncomfortable paradoxes which allow its communication to occur in the first place. In other words, there are only concrete methods of effective procedure which unavoidably *propagate* the view that *all* problems can be totally solved in advance.

Then again, perhaps Turing wasn't exactly prophetic in calling it propaganda considering his contributions to cryptography and the mathematical work of decoding encrypted messages. There is a lot more going on in Turing's definition of propaganda than passing it off as an anachronism. For instance the historical relationship between Turing's contribution to decoding the enigma code for the Government Code and Cypher School (the forerunner of GCHQ) continues to play itself out in the ongoing NSA mass surveillance revelations (Hopkins). This seventy year history does not just capture the secret relationship between two regimes of state surveillance, *but how the propagation of mathematical proofs decide ideological effects*. Indeed, a detailed account of how the NSA actually managed to enact such surveillance, is implicated in the ecologies of problem solving and formalising proofs, just as it was for Bletchey Park. Both ecologies establish similar propagative strategies but with different historical principles.

In September 2013 Edward Snowden's leaked a number of NSA memos, which showed exactly how the NSA managed to hack into personal accounts, emails and messages. They were completely reliant on the demonstration of one single mathematical proof which relied on solving an equation. The proof in question lay in a public key encryption algorithm, entitled a *Dual Elliptic Curve Deterministic Random Bit Generator* (Dual_EC_DRBG) introduced by the National Institute of Standards and Technology (NIST) in 2005 as the national standard for web encryption (Barker and Kelsey).

Elliptic Curve Cryptography (ECC) is an entire industry in mathematics specialising in encrypting messages using modular arithmetic and large number factorisation formulae. Sending messages are easy to encrypt, but mathematically improbable to decrypt, unless you have the necessary private key. Along with other public key encryption methods (such as RSA), ECC's use has almost single handily contributed to the relative stability of internet security infrastructure: securely transmitting digital messages, emails, tweets, data, bit coin and bank transactions all through a public infrastructure. ECC and RSA have *constructed a decision ecology of a supposedly secure web*.

It is the reliance of mathematical proofs which matter here. ECC affords the sender to encrypt a message using public and private integers, or keys, which are created by multiplying huge prime numbers. The receiver can decode the message on the same basis.

In order to illegally hack and decrypt such encryptions without having access to the decoding private number, it is necessary to factorise the public number into its original primes. Because such factorisations are hard or intractable (i.e. infinitely possible,

but finitely impossible using current computational means), the hardness of the mathematical problem establishes the security of the transmission. Here we can see that moderately unsolvable mathematical problems are actually responsible for encrypting secure messages.

ECC works by plotting a curve where two solutions (y and x) exist to satisfy a simple equation. Dual_EC_DRBG uses the following equation (where b is an integer and [mod p] is the prime number used):

$$y^2 = x^3 - 3x + b \pmod{p}$$

Thus, the plot lines on the elliptical plane curve correspond to the private and public solutions which generate large numbers for encryption. The Dual_EC_DRBG algorithm, creates pseudo random numbers which look publicly random next to the curve, but can be securely decrypted.

However, Snowden's leaked memo showed that NIST propagated Dual_EC_DRBG with the full knowledge that NSA developed a back door within the algorithm itself (speculation suggests that the NSA explicitly paid RSA £10 million to support the insecure algorithm). Essentially, NSA propagated a mathematical proof inherent to Dual_EC_DRBG which allowed them to decrypt any encryption produced, so long as the Dual_EC_DRBG was used as a general standard: which it was, as in the case of Microsoft (Windows Vista and Windows 7/8), Cisco systems, IBM, Blackberry, Symantec, to name just a few (DRBG Validation List). Before Snowden leaked anything, there was already some suspicion of Dual_EC_DRBG back in 2007 (Schneier), where it was shown the numbers defining the elliptic curve had never been disclosed. Two Microsoft researchers (Shumow and Ferguson), showed that these numbers correlated to a second hidden set of numbers, which if known would solve Dual_EC_DRBG's intractability thus having, quoting Schneier, "the keys to the kingdom."

Indeed, Dual_EC_DRBG appears to be have been propagated as an infrastructure which supports only one direction of encryption, because NIST produced *the* public document recommending it as *the* standard. Such calculable mathematical proofs *operationalise* devious exercises of propagation, which in this case, constructs an entire security infrastructure concealing back doors for surveillance. What is important to note is that this propagated back-door is a bona-fide mathematical proof: inherently effective.

Thus, what is computation if it isn't the technical means of enacting effective, efficient, propagated pre-determined results through societal means? What if the machine was the propagandist? Propaganda largely avoids intractability: it can't stand it. Difficult questions cannot be decided. Frederic Charles Bartlett argued that propaganda was primarily a *decisive* method of suggestion, not simply designed to control psychological behaviour, but to acquire specific, *effective* results through purposeful action (Bartlett). Perhaps we could add to this, the deeper realisation that propaganda is no longer limited to the limits of psychological behaviour, or the limits of societal communities, but extends to the mathematical limits of decisional machines which decide results in a real infrastructure. Ideology no longer operates at the borders of human knowledge, but of automated systems.

Propaganda is part and parcel of computational culture and of technical infrastructure: not just posters, pamphlets, zines and broadcasts, but now, gamification, platform devices, spy-ware, pseudorandom encryption algorithms, services and subscriptions. Each one only allows certain pre-determined outcomes to be realised and exploited. Each

one already deciding (or propagating), a limited number of routes, which users mistake for their own 'openness'. If there is one thing Silicon Valley or the NSA would love to solve, in their self-congratulatory wallowing, it is detecting whether a certain problem always has a provable solution: and whenever they come up with one, it usually has a market to satisfy and a propagative strategy to make it seem beneficial.

In this post-digital realisation, information doesn't seem to want to be free (Polk): or at the very least, it wants to convince you it might be. Digital information simply wants to propagate itself as a watchdog for any problems that are always-already resolved, refusing its own transparency in turn. The best we can hope for is to understand information's propagative effect, and ask not of its truth, but of what it propagates. Following Orwell, we should admit that as far as the post-digital is concerned, "[a]ll propaganda is lies, even when one is telling the truth. I don't think this matters so long as one knows what one is doing, and why" (Orwell, Davidson & Angus 229).

Works cited

Althusser, Louis. "Ideology and Ideological State Apparatuses (Notes Towards an Investigation)". In *Lenin and Philosophy and Other Essays*. Translated by Ben Brewster. New York: Monthly Review Press. 1971. pp. 127-186. Print.

Barker, Elaine and Kelsey, John. "Recommendation for Random Number Generation Using Deterministic Random Bit Generators". NIST Special Publication 800-90A, January 2012. Web. <http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf>

Bartlett, Frederic C. *Political Propaganda*. Cambridge: Cambridge University Press. 1940. Print.

Berry, David. M. *The Philosophy of Software: Code and Mediation in the Digital Age*. London: Palgrave Macmillan. 2011. Print.

Brady, Anne-Marie. *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China*. Lanham MD: Rowman & Littlefield. 2008. Print.

Church, Alonzo. "An unsolvable problem of elementary number theory". *American Journal of Mathematics*. Vol 58. 1936. pp. 345–363. Print.

Cramer, Florian. "Post-digital: a term that sucks but is useful (draft 2)." *Post-digital Research*. Kunsthal Aarhus. Oct. 7-9, 2013. Web. <http://post-digital.projects.cavi.dk/?p=295>

Cunningham, Stanley. B. *The Idea of Propaganda: A Reconstruction*. Praeger: Westport, 2002. Print.

Daugherty, William. J. "The creed of a modern propagandist". In *A Psychological Warfare Casebook*. Edited by William. J. Daugherty and Morris Janowitz. Baltimore: John Hopkins University Press. 1958. Print.

National Institute of Standards and Technology (NIST). "DRBG Validation List", last updated January 10th, 2014. Web. <http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html>

Ellul, Jacques. *Propaganda: The Formation of Men's Attitudes*. Trans. Konrad Kellen & Jean Lerner. New York: Random House, 1973. Print.

Ewes, Richard. "The world maker." *New Scientist*. Aug. 11, 2012. pp. 33-37. Print. Also published in; Ewes, Richard. "The Algorithm that runs the world." *New Scientist. Physics & Math*. Aug. 13, 2012. Web. <http://www.newscientist.com/article/mg21528771.100-the-algorithm-that-runs-the-world.html?page=1>

Galloway, Alexander. *Protocol: How Control Exists After Decentralization*. Cambridge: MIT Press. 2004. Print.

Gandy, Robin. "Church's Thesis and the Principles for Mechanisms". In *The Kleene Symposium*. Edited by H.J. Barwise, H.J. Keisler, and K. Kunen. North-Holland Publishing Company. 1980. pp. 123–148. Print.

Gass, Saul. I, & Assad, Arjang. A. *An Annotated Timeline of Operations Research: An informal History*. New York: Kluwer. 2005. Print.

Golumbia, David. *The Cultural Logic of Computation*. Harvard: Harvard University Press. 2009. Print

Good, Irving J. "Studies in the History of Probability and Statistics. XXXVII A. M. Turing's Statistical Work in World War II". *Biometrika*, Vol. 66: No. 2. 1979. pp. 393–396. DOI: 10.1093/biomet/66.2.393. Print.

Grimmelmann, James. "Some Skepticism About Search Neutrality", in *The Next Digital Decade: Essays On The Future of The Internet*. Edited by Berin Szoka and Adam Marcus. Washington D.C: Tech Freedom. 2010. pp. 435 – 460. Print.

Hilbert, David. 'Probleme der Grundlegung der Mathematik' [Problems Concerning the Foundation of Mathematics]. *Mathematische Annalen*. Trans. Elisabeth Norcliffe. 102. (1930). 1-9. Print.

Hopkins, Nick. "From Turing to Snowden: how US-UK pact forged modern surveillance", *Guardian Online: The NSA Files: Decoded.* Dec. 2, 2013. Web. <http://www.theguardian.com/world/2013/dec/02/turing-snowden-transatlantic-pact-modern-surveillance>

Kenez, Peter. *The Birth of the Propaganda State: Soviet Methods of Mass Mobilization 1917 – 1929*. Cambridge: Cambridge University Press. 1985. Print.

Morozov, Evgeny. *To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems that Don't Exist*. London: Allen Lane (Penguin). 2013. Print.

Orwell, George. Davison, Sheila & Angus, Ian. *All Propaganda is Lies, 1941 – 1942*. London: Random House. 2001. Print.

Polk, Wagner. R. “Information Wants to Be Free: Intellectual Property and the Mythologies of Control”. *Columbia Law Review*, Vol. 103, May 2003; U of Penn, Inst for Law & Econ Research Paper No. 03-22; U of Penn Law School, Public Law Working Paper No. 38. Also available in Polk, Wagner. R. “Information Wants to Be Free: Intellectual Property and the Mythologies of Control”. Print. SSRN: <http://ssrn.com/abstract=419560> <http://dx.doi.org/10.2139/ssrn.419560>

Price, Robert & Shannon, Claude. E. “Claude E. Shannon: An Interview Conducted by Robert Price”. IEEE History Center, Interview #423. 28 July, 1982. Interview (Audio file).

Rosser, John. B. “An Informal Exposition of Proofs of Gödel’s Theorem and Church’s Theorem”. *The Journal of Symbolic Logic*. Vol. 4, No. 2. 1939. pp. 53–60. Print.

Schneier, Bruce. “Did NSA Put a Secret Backdoor in New Encryption Standard?”, *Wired Commentary*. Nov. 15, 2007. Web. <http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115>

Shannon, Claude E. *A Mathematical Theory of Communication*. Bell System Technical Journal, Vol. 27. 1948. pp. 379–423, 623–656. Print.

Shumow, Dan and Ferguson, Niels. “On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng”. RYPTO Rump Session. 2007. Microsoft. Web. <http://rump2007.cr.yp.to/15-shumow.pdf>

Tehran Times, “Transcript – Confessions of the arrested CIA spy aired on Iranian TV,” Political Desk, *Tehran Times* Website. Dec 18, 2011. Web. <http://www.tehrantimes.com/politics/93662-transcript-confessions-of-the-arrested-cia-spy-aired-on-iranian-tv>

Turing, Alan.”On Computable Numbers, with an Application to the Entscheidungsproblem”, *Proceedings of the London Mathematical Society*, Series 2, 42 (1936-7), pp 230–265. Print.

Turing, Alan. “Solvable and Unsolvable Problems.” In *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life: Plus Secrets of Enigma*. Edited by Jack Copeland, (Oxford: Oxford University Press, 2004), pp. 582-595. Print. Originally published as Turing, Alan. “Solvable and Unsolvable Problems.” *Science News*. No. 31. (1954) pp. 7 – 23. Print.

Zielinski, Siegfried. *[After the Media]: News from the Slow-Fading Twentieth Century*. Minneapolis: Univocal Publishing. 2013. Print.