# Words For A Wired World: Cybersecurity As Communicative Art

**ABSTRACT:**

In this paper I propose to examine the Snowden affair as a cultural and communicative phenomenon, looking at the ways in which the discussions around it have been framed and presented by his supporters, his detractors, and by Snowden himself. Drawing on a range of texts, but focusing primarily on the 2014 graphic novel "Beyond Edward Snowden", Snowden's 2014 TED talk and the response to this by NSA deputy director Richard Ledgett, I will seek to present a study which, drawing on Critical Discourse Analysis, corpus linguistics and Lakoff's theories of "frames", allows us to better understand the ways in which this event has been "read" by the various sides.

The Snowden case exemplifies the challenge faced by those working within cybersecurity to present their activities (above all those which involve the monitoring of the general public and the capture of data concerning them) in a way which appears reasonable and truthful, and which is expressed in a way which matches the vision of the world held by the intended audience. In a climate of ever-growing distrust of officialdom and government in general, there is a desperate need to find a more effective manner of stating the case against the actions of individuals such as Snowden, Manning, and Assange (to say nothing of the activities of groups such as Anonymous). The metaphor of cybersecurity as a war is both powerful and valid, but it is a conflict where the weapons must be both technical and verbal.

## Words For A Wired World: Cybersecurity As Communicative Art

### 1. Introduction: Shaping the Terrain

"Nothing 'is'" (Morrison (1997): 12)

[*Author's Note: Throughout this paper, I will be referring to the texts examined as examples of "discourse"; what this term means depends on who is using it, and why. A Foucauldian uses it to mean a text which exemplifies (often implicit) sociocultural power relations, while a linguist engaged in discourse analysis (not Critical Discourse Analysis) uses it to mean a text of substantial length, under analysis to examine its syntactic, lexical and semantic features. My definition of the term is perhaps closest to that given by the Critical Discourse Analyst Norman Fairclough (2015): "discourse is language in relation with other elements in the social process." (8). In other words, "discourse" should be read here as synonymous with "a text inscribed within, spring from, and embodying a particular set of social, cultural and ideological values".]*

In a 2004 *New Yorker* article, Malcolm Gladwell discusses the career of the marketing guru Howard Moskowitz, who was asked by Pepsi to undertake research to determine the "ideal" level of sweetener for their diet cola. Moskowitz argued that the secret to success in product design lay in the construction of a range of products, rather than the creation of a single "one size fits all" brand. As Gladwell (2004) puts it, ""There was no such thing as the perfect Diet Pepsi. They should have been looking for the perfect Diet Pepsis." What Moskowitz says about cola, or spaghetti sauce, or coffee is equally true of our domain; there is no such thing as perfect cybersecurity – we should be looking for the perfect cybersecurities. The idea of a single tactic or set of protocols to counter the range of threats and vulnerabilities in informational space is ludicrous; we cannot mitigate against insider threat or social engineering in the same way that we defend against DDOS attacks or ransomware. Technical issues require technical solutions; my interest lies in the human aspect of the domain, and in particular in this paper I wish to examine the way in which cybersecurity exists within the wider realm of human discourse, an informational space which is bounded and shaped by politics, ideology and culture as much as by technology. For cybersecurity to be truly effective, it must adopt a blended approach, drawing on as wide a range of disciplines as possible; as Wiener (1988) puts it, "There is no Maginot Line of the Brain" (122); what follows is an attempt to address certain aspects of human behavior which have an inevitable influence on the work of the cybersecurity professional, both directly and in terms of shaping the environment in which he or she seeks to operate.

As with any sphere of human activity, cybersecurity exists not just as a thing in itself, a clearly-defined discipline and set of interests, but as a cultural artefact, open to opinion,

interpretation, and misinterpretation. The problems this raises with regard to any consideration of "trust" should be obvious; for something to be trusted, it must be accepted as congruent with the beliefs of the individual or group to whom it is presented, and this is never a matter of logic alone. The idea that humans make decisions on coldly rational grounds is fatally flawed, as Chatfield (2009) points out:

> Over the past two decades, economists have been rediscovering human behaviour—real, irrational, confusing human behaviour, that is, rather than the predictable actions of the "economic man" who used to be pressed into service whenever modelling was to be done.

If we are to successfully promote tactics and policies which we believe will lead to a more secure cyberdomain, then it must be done in a way which matches what we know about the processes which successfully influence human behaviour at both an individual and cultural level.

Consider the following diagram, with which generations of linguists are all-too familiar:


**Figure 1**: Saussure's model of a human speech act (Saussure (1985): 27)

Saussure presents here an idealized model of human communication, where an idea passes from the mind of speaker A to the mind of hearer B via the channel of speech; this in turns leads to a response transmitted from B to A. The connections between this model and the Shannon Weaver model of wireless communication are obvious, and as with any model, it serves a useful purpose in reducing the act to its essentials; except of course it does not. As a model of human communication in reality, it neglects the essential fact that these actions do not take place in a neutral zone, uninfluenced by any external factors. True human language, in short, is "noisy". More than that, the terrain of discourse is not a level plane, but a zone contoured by hierarchies and power relationships; Saussure places both speakers on the same level, and this is almost never the case in any real human communication. If we are to generate trust, we need to consider what Pratkanis (2007) terms "landscaping", presenting our arguments in ways which enable us to "occupy the moral high ground" (the metaphor is entirely apt). We must consider not just the *content* of our communication, but its *form*; in short, we need to be aware of the way in which our information is *framed*.

We know from a series of experimental studies, building on the groundbreaking work of Loftus and Palmer (1974), that language can have a direct effect on cognitive processes

such as memory; Hirschman, Kahneman *et al.* (1983) discuss the ways in which human decision making is invariably conditioned by pre-existing mental heuristic frameworks and the way in which the choice is presented. The same is also true of the wider domains of political debate and persuasion in general. We view the world through a series of filters, which are formed by education, family and peer group influences and wider ideological elements; these filters construct our mental map of creation, the frame within which we operate. Much work on political communication foregrounds the importance for those who wish to form opinions to rely on this concept of *framing*, that process by which:

> a speaker's emphasis on a subset of potentially relevant considerations causes individuals to focus on these considerations when constructing their opinions (Druckman (2001): 1042)

All human thought and communication is framed; a means of exerting effective influence (and for increasing the likelihood that messages will be trusted) is to ensure that we deliberately communicate in a way which matches our audience's frame. The work of George Lakoff has been invaluable in showing the importance of an understanding of the concept of framing as a *sine qua non* for successful communication; medium and message must work together:

> Framing is about getting language that fits your worldview. It is not just language. The ideas are primary – and the language carries those ideas, evokes those ideas. (Lakoff (2004): Chapter 1.)

What I want to emphasize above all in this paper is that we cannot hope to gain the trust of users if we do not present what we do in a way which makes sense to them, and which chimes with their innate conception of the way the world is/should be. Such an approach requires the use of tools and approaches drawn from linguistics, as a means of determining the ways in which communication is innately linked to and inscribed within extant cultural frames. In what follows, I will be drawing on two specific methods of linguistic enquiry. Firstly, **critical discourse analysis (CDA)**, which, as Norman Fairclough (2015) puts it:

> combines **critique** of discourse and explanation of how it figures within and contributes to the existing social reality, as a basis for **action** to change that existing reality in particular aspects. (6)

CDA offers a way of examining texts as a means of revealing their underlying sociocultural and ideological drivers, and can be immensely powerful. However, it should be noted that (a reflection of CDA's origin in the radical left-wing scholarship of figures such as Marcuse and Foucault) Fairclough presupposes that the "existing social reality" *should* be changed. One of the great dangers of CDA is that it can lead to analyses which are *a priori*, *parti pris* and partial, in both senses of the term (incomplete and prejudiced). To be truly valuable, and to defend the activity against accusations of unfounded speculation, CDA must be grounded in empirical data, and base its conclusions on a bedrock of testable evidence.

Such evidence can, I believe, be provided by recourse to the second of the analytical approaches I will be employing here, namely **corpus linguistics (CL)**. This takes a text or texts, which form the **corpus** to be investigated, converts them to a machine – readable form (in this case UTF-8 encoded .txt files), and analyses them through the use of various tools in order to reveal significant details concerning word frequency, collocation and to create concordances of keyword appearance. (The software used in this paper is AntConc (v.3.4.3), a freeware program devised by Laurence Anthony). What might be termed the "CDA community" has shown a certain reluctance to embrace CL (Fairclough (2015): 21), but I believe that it can be more than a starting point for enquiry, rather an invaluable and inescapable part of the process of a data-driven CDA. My opinion here chimes is perfectly expressed by Baker *et al.* (2008):

> to show that neither CDA nor CL need be subservient to the other […] but that each contributes equally and distinctly to a methodological synergy. (274)

Having now outlined this paper's critical stance, and the methodological approach it seeks to follow, we must now consider the material I wish to examine. Given that a central element of my argument is that "cybersecurity" must engage with opinion and perception as much as with fact, I will be looking at a case study which exemplifies the problems, namely the case of Edward Snowden. I am not concerned with *what* he did, or *how* he did it (these are technical matters, and lie outside my area of expertise); rather, what matters here is what we might term the "meaning" of his actions, and the way in which they have been presented to and perceived by the general public. This is a difficult, complex, and contentious subject, but it must be examined if we are to truly understand how cybersecurity operates within society and culture. The problems are exemplified by the cover of the September 2014 issue of *Wired*; aimed at an audience of IT-savvy, would-be opinion-formers and digital natives, the magazine is a forum in which the cybersecurity agenda is repeatedly presented and examined – but not in ways that the cybersecurity establishment will find comfortable. According to NSA director Keith Alexander, Snowden has done irreparable damage to the security of the United States:

> "This is an individual who is not acting, in my opinion, with noble intent ... What Snowden has revealed has caused irreversible and significant damage to our country and to our allies." (Ackerman and Rush (2013)).


**Figure 2**: Snowden as icon (Wired)

That is most definitely *not* how *Wired* depict him; consider the iconography of the image. A young man, thin, ascetic, with close-cut but carefully coiffed hair and unshaven stubble, stares soulfully into the middle distance, his eyes not meeting the reader's, but gazing above and beyond. The presentation is not that of a traitor, but a mystic, or a saint (and martyr?); the religious resonances are undeniable, and arguably deliberate. It is surely no accident that the photo has been lit to give Snowden a halo. To further counter the idea of Snowden as traitor, he is depicted holding, not burning or tearing, the American flag; I would ask the reader to consider whether it is being held as a lover or as a child (I veer towards the latter). Whichever it may be, he is undeniably cradling it as something to be respected, loved, and protected, entirely in accordance with the guidelines of the US Code, Title 4, § 8. "Respect for Flag":

> No disrespect should be shown to the flag of the United States of America

and § 8 (j):

> The flag represents a living country and *is itself considered a living thing*.
>
> [my emphasis]

It must be noted that *Wired* is owned by the Condé Nast publishing empire, which produces other entirely mainstream magazines as *Bon Appétit*, *Brides*, *Golf World*, and

*The New Yorker*; it does not spring from a hotbed of political radicalism, and relies for its survival on capturing the largest possible readership. When a magazine like *Wired* presents Snowden in this way, it is clear to see that those in our community who seek to present the activities of the government and state security services as trustworthy have an uphill task. As Paul Newman puts it in *Cool Hand Luke* (1967), "What we got here is a failure to communicate." Shortly after saying this, his character is repeatedly shot; this seems to me a powerful symbolic representation of the risks we run if we fail to find a way to engender trust in what we do. The Snowden affair will, I believe, be seen as a key event in the history of the development of cyberspace as technical environment, human habitat and political battleground. In what follows I want to examine how its presentation may offer possible paths for study as ways of shaping this new terrain.

## 2. Cybersecurity as Performance: Analysing Snowden and Ledgett

Since its initial meeting in 1984, leading to the establishment of annual conferences in 1990, TED (Technology, Entertainment, Design) has set out to be the event of the year for those who see themselves as the movers and shakers, innovators and opinion formers of the modern world. In their own words:

> TED is a global community, welcoming people from every discipline and culture who seek a deeper understanding of the world. We believe passionately in the power of ideas to change attitudes, lives and, ultimately, the world. (ted.com (2015)).

This self-selected assembly of the great and good ensure that the addresses at their meetings are distributed as widely as possible, via their website, a YouTube channel and apps for both IOS and Android. The list of TED speakers is an alphabet of all the talents, from Isabel Allende to Ray Zimbardo, taking in on the way a catalogue of celebrity, science and commerce: Bono, Bill Gates, Bill Clinton, Brian Eno, David Cameron, Jimmy Wales, Sergey Brin… and so on. Our interest here lies in two talks which took place at TED 2014, on March 17 and 19 respectively. On these dates, TED pulled off a duo of *coups de théâtre*; without any prior warning, they staged presentations by both Edward Snowden, at that time arguably the most-wanted man in the world, and the Deputy Director of the NSA, Richard Ledgett.

From the perspective of a CDA-based study of these addresses, we must initially move away from a consideration of their content, and consider the general environment in which they occur; TED is not a court of law, and we would not expect the speakers to be subjected to a forensic level of questioning, or even the robust, combative of style of interrogation seen in news broadcasting; this is undoubtedly the case here. Both Ledgett and Snowden are treated with respect by their questioners, and to those of us accustomed to the interviewing style of, say, Jeremy Paxman, they seem to get off very likely. This is particularly true in the case of Snowden, who is given an extremely easy ride.(One of the areas for future research in this area will be an analysis of the interview Snowden gave to NBC's Brian Williams, where he seems, on the basis of an initial examination, to be treated equally gently). What we see here is not an inquisition, but a forum where both sides in the affair can state their case, and the audience (both in the hall and in the wider world) are left free to draw their own conclusions, solely on the

evidence of the speakers' own words; at least, that is the theory. I would argue that what we actually see here is a framing (whether deliberate or unconscious is open to question) which subtly prejudices the viewer towards regarding Snowden as the injured party. As I have said, at no point is he really put on the spot, and it is significant that one of his questioners, who explicitly states his positive view of Snowden's actions is Tim Berners-Lee. When the creator of the World Wide Web places himself in your camp, you are clearly not in hostile territory.

A further element of presentational slant can be seen in the way the speakers are presented; neither Snowden nor Ledgett is actually physically present at the venue (the reasons for this are not difficult to determine in Snowden's case). Both appear as "talking heads", projected on screen so the audience can both hear and see them; the history of broadcasting shows us how important image can be in the transmission of ideas in the battle to win over an audience. Consider the classic case of the Kennedy/Nixon debate; under the studio lights, Nixon appeared sweaty, unshaven, and his grey suit looked bleached out and insubstantial, while Kennedy, who wore a dark suit and make up, appeared composed, assured and solid. However, those who heard the debate on radio, and were not distracted by the images, overwhelmingly gave the day to Nixon. What we see at TED is a similar process of presentational framing: Ledgett appears as a projected, magnified image, as does Snowden, but the presenters also allow Snowden another mode of presence, combining the virtual and the actual. When introduced, from the back of the hall emerges a mobile monitor, mounted at approximately head height, on which is projected the face of Snowden, a live image in quasi-human form. The telepresence robot moves to the front of the stage and begins to interact with the convenor and the audience (the robot has a camera, which allows Snowden to see the hall in real time). Snowden effectively appears before the audience "in person", or as much in person as he is allowed to; he is *embodied*, given a concrete presence on a human scale which is denied Ledgett. I would argue that this deliberately loads the bases in Snowden's favour, not least because it heightens the sense that his true presence in the flesh is denied to us; his appearance in robotic form simply reinforces the idea that he is not permitted to appear free and unconstrained to state his case in person. One wonders why the same courtesy was not extended to Ledgett.

The presentational form, then, can be seen to tip the scales in Snowden's favour; turning to the actual content of what the two men say, what can be determined? Firstly, it must be noted that what we are witnessing here is effectively performance; we are not presented with a neutral dataset which we are free to interpret as we might wish. Rather, the men are seeking to advance their own opinion as the "truth", and as such, any audience must take into account the centuries of work on poetry and rhetoric, the art of persuasion and influence but the power of spoken language. Aristotle defined rhetoric as "the faculty of observing in any given case the available means of persuasion." (Rapp (2002)) He argued that it rests on three essential elements: **ethos** (the personal qualities of the speaker or the person or body promoted or attacked), **pathos** (the appeal to emotion) and **logos** (the use of reason, and factual evidence). What we see here are two examples of discourse which deploy all three of these tactics. Both speakers present (or claim to present) factual evidence to justify their point of view. Ledgett gives figures for the numbers of terrorist attacks prevented by NSA surveillance, whilst Snowden claims that "secret judges in a secret court based on secret interpretation of law" (Snowden (2014**a**) - note the rhetorical device of repetition to

foreground ”secret”, and by extension unaccountability - have approved tens of thousands of government warrants. However we can again see that the way in which the speakers are presented to the audience gives Snowden’s arguments an added weighting of ethos and pathos; he is framed as the lone crusader for justice, an exile from his own country, claiming that all his actions have been motivated by that most essential of American values, love of country, and a simple desire to do what is right:

> If I had to describe myself, I wouldn’t use words like ”hero.” I wouldn’t use ”Patriot,” and I wouldn’t use ”traitor.” I’d say I’m an American and I’m a citizen, just like everyone else. (Snowden (2014**a**)

We cannot neglect the importance of ethos and pathos as persuasive tools; Snowden’s words tap into centuries of American mythologizing about the heroic individual battling institutional injustice and the authoritarian force of ”big government”. His self-deprecating tone is straight out of a Frank Capra film; *Mr Snowden goes to Washington*, as it were. Note that the recent documentary on the Snowden affair is titled *Citizenfour*; again we have the idea presented that he is one of us, and an ”Us” who must fight against an implicit “Them”.

This, then, is the general context within which the two texts operate, and CDA can permit us to take it much further, showing how Snowden presents himself as the voice of American individualism. Conversely, Ledgett is restrained by the fact that he speaks for the establishment, the mouthpiece of the ”security state”; the fact that Ledgett speaks not as an individual, but on behalf of the organisation for which he works, is further weakens any attempt to form a rapport with his audience. We live in an era where distrust and suspicion of government and the organs of the state are rife, and anyone who speaks for the NSA in the wake of the disclosures of Snowden, Manning and Assange is inevitably going to be seen as compromised. Whether this is fair or accurate is beside the point; this is simply how it is. What we could term ”the plane of discourse” within which discourses about cybersecurity occur has been shaped (some might say deformed) by these disclosures, and any attempt to ignore this or discount it is pointless. In trying to present the official response to Snowden, Ledgett is faced with the near impossible task of persuading his audience (and the wider world) that the official line is the right one. This is, I would argue, a big ask.

What is presented here is very much a preliminary study, which I am reluctant to dignify even with the description ”work in progress”; it represents merely an attempt to sketch out an initial methodology for the investigation of the Snowden affair, and to be truly valid, there is a need to consider a much broader range of texts where Snowden’s actions are discussed and debated in the public sphere. In many ways, this is a preliminary proof of concept, the attempt to see whether an investigative approach based on the combination of CDA and CL can obtain significant data about the way in which cybersecurity can and should be presented. A CDA-based approach clearly has much to offer in terms of showing how the way in which our arguments are advanced is an essential consideration.  What can a closer analysis of the actual language used by Snowden and Ledgett offer?

Given that these two speakers represent completely opposite positions, the first thing to note is how similar to the language they use actually is. An analysis of lexical frequency

reveals a close degree of similarity between the ways in which they coached the arguments, as table 1 shows.(I have merely listed the first 50 words used by both in order of frequency).

| | Snowden | Ledgett |
|---|---|---|
| 1 | the | the |
| 2 | to | that |
| 3 | that | and |
| 4 | and | of |
| 5 | of | to |
| 6 | a | in |
| 7 | i | a |
| 8 | we | s |
| 9 | in | is |
| 10 | s | we |
| 11 | is | i |
| 12 | it | are |
| 13 | they | so |
| 14 | not | have |
| 15 | t | it |
| 16 | but | there |
| 17 | this | you |
| 18 | you | those |
| 19 | be | think |
| 20 | for | our |
| 21 | have | for |
| 22 | are | people |
| 23 | re | they |
| 24 | there | re |
| 25 | about | who |
| 26 | these | one |
| 27 | by | on |
| 28 | can | not |
| 29 | nsa | actually |
| 30 | our | do |
| 31 | what | them |
| 32 | government | with |
| 33 | people | about |
| 34 | just | other |
| 35 | world | t |
| 36 | an | by |
| 37 | do | or |
| 38 | ve | things |
| 39 | with | but |
| 40 | been | their |
| 41 | going | way |
| 42 | has | all |
| 43 | internet | be |
| 44 | was | been |

| | | |
|---|---|---|
| 45 | need | information |
| 46 | think | nsa |
| 47 | when | work |
| 48 | all | he |
| 49 | as | like |
| 50 | because | some |

**Table 1**: Comparison of lexical frequency in the Ledgett and Snowden TED talks.

This, however, should come as no surprise; CL will inevitably reveal that in normal speech, the most frequently used words will tend overwhelmingly to be articles ("the","a". ..), determiners ("the", "this", "those"…) and verbs(e.g. forms of the copular such as "is" and "are" and common verbs such as "can" and "have"). A comparison of these texts with a list of lexical frequency derived from COCA (the Corpus of Contemporary American English, available for consultation at http://corpus.byu.edu/coca/) shows just "typical" both speakers' language use is. (see Table 2 below).

| | Snowden | Ledgett | COCA |
|---|---|---|---|
| 1 | the | the | the |
| 2 | to | that | be |
| 3 | that | and | and |
| 4 | and | of | of |
| 5 | of | to | a |
| 6 | a | in | in |
| 7 | i | a | to |
| 8 | we | s | have |
| 9 | in | is | to |
| 10 | s | we | it |
| 11 | is | i | I |
| 12 | it | are | that |
| 13 | they | so | for |
| 14 | not | have | you |
| 15 | t | it | he |
| 16 | but | there | with |
| 17 | this | you | on |
| 18 | you | those | do |
| 19 | be | think | say |
| 20 | for | our | this |
| 21 | have | for | they |
| 22 | are | people | at |
| 23 | re | they | but |
| 24 | there | re | we |
| 25 | about | who | his |
| 26 | these | one | from |
| 27 | by | on | that |
| 28 | can | not | not |
| 29 | nsa | actually | n't |

| | | | |
|---|---|---|---|
| 30 | our | do | by |
| 31 | what | them | she |
| 32 | government | with | or |
| 33 | people | about | as |
| 34 | just | other | what |
| 35 | world | t | go |
| 36 | an | by | their |
| 37 | do | or | can |
| 38 | ve | things | who |
| 39 | with | but | get |
| 40 | been | their | if |
| 41 | going | way | would |
| 42 | has | all | her |
| 43 | internet | be | all |
| 44 | was | been | my |
| 45 | need | information | make |
| 46 | think | nsa | about |
| 47 | when | work | know |
| 48 | all | he | will |
| 49 | as | like | as |
| 50 | because | some | up |

**Table 2**: Comparison of lexical frequency in the Ledgett and Snowden TED talks with normal frequency in US English, as derived from COCA.

Such data is helpful, not so much for what it reveals about the communicative styles of Snowden and Ledgett, but for those who wish to communicate with the general audience; we must present information in a way which appears conventional and familiar; trust is engendered by communication which matches the expectations of an audience.

Returning to the examples under analysis, a simple frequency analysis is less than helpful when seeking to determine the specifics of their communication. Of more use is a study of the **keywords** within the texts, i.e. those words which are used more frequently than is the norm. Such an analysis is performed by mapping a text against a corresponding corpus of texts which matches the time period and language zone where the texts examined originate. As I do not currently have access to the full COCA dataset, I have used here MASC (the Manually Annotated Sub-Corpus, available at http://www.anc.org/data/masc/), a freely available dataset of contemporary American English written and spoken data derived from the Open American National Corpus (OANC); MASC, dating from 2006, contains a balanced set of 50, 000 words drawn from a wide range of spoken and written sources, and provides an appropriate bass for this proof-of -concept study.

The keyword analysis reveals the following data (listing the top 20 keywords only); put crudely, if frequency analysis tells us what people are talking *about*, keyword analysis analyses to get a data-driven insight into what really *matters* to them.

| | Snowden | Ledgett |
|---|---|---|
| 1 | **nsa** | **that** |
| 2 | **internet** | **nsa** |
| 3 | **that** | so |
| 4 | government | those |
| 5 | **we** | actually |
| 6 | **intelligence** | **privacy** |
| 7 | **communications** | **metadata** |
| 8 | prism | **intelligence** |
| 9 | they | think |
| 10 | **metadata** | there |
| 11 | **privacy** | **we** |
| 12 | these | **communications** |
| 13 | world | are |
| 14 | programs | capabilities |
| 15 | companies | allies |
| 16 | re | inspector |
| 17 | bullrun | transparent |
| 18 | intercepted | have |
| 19 | secret | **internet** |
| 20 | ve | snowden |

**Table 3**: Keyword comparison of Snowden and Ledgett talks (using MASC as a base corpus for analysis) – common terms in bold.

What we see here, as before, is that the two speakers share a common set of interests, albeit with significant differences. To cite only one example; Snowden refers to PRISM and BULLRUN, which he claimed (on the basis of the information he leaked to the press) to be programs for respectively mass surveillance and decryption of electronic communications. Ledgett, makes no mention of BULLRUN whatsoever, and mentions PRISM only to deny that it was used against the US population in general. If we wish to understand in detail the differences in position between the two men, we must turn to another key tool of CL, and consider not just the individual keywords, but their **collocations**, i.e. the words which appear in proximity to the keywords. An oft-cited dictum of CL is that "you can tell a word by the company it keeps"; automated collocation analysis allows us to detect these ties with ease.

Purely for the sake of example (and remembering as ever that this is a proof-of-concept study), I present below the results of a search via Ant Conc for collocations in the two texts with the keyword "NSA". It is hardly surprising that both Snowden and Ledgett attach such an importance to the word (as evidenced by the high degree of "keyness" it possesses in both texts; what must be noted is that a study of the phrase's collocations allows us to easily see that the two speakers adopt very different stances towards the national Security Agency. If we examine the collocations of "NSA" in Ledgett's talk (see Table 4 below), then can see that the term is rarely if ever used in a negative light, and when it is (as in collocation 5 below, it is not arguing for moral or ethical shortcomings, but to suggest that it has simply failed to display openly that it is acting ethically.

| | | | |
|---|---|---|---|
| 1 | So what if somebody who works in the | NSA | -- and there are over 35,000 people who do. |
| 2 | Mr. Snowden, he had the option of the | NSA | inspector general, the Navy inspector general, |
| 3 | that he's disclosed, the capabilities, and the | NSA | is a capabilities-based organization, so when |
| 4 | space. But I will tell you this. So | NSA | has two missions. One is the Signals Intellige |
| 5 | our processes, our oversight, who we are. We, | NSA | ,have not done a good job of that, |
| 6 | in terms of numbers of terrorist attacks that | NSA | programs contributed to stopping was 54, 25 of |
| 7 | beating the heck out of us over the | NSA | programs, by the way. So that's not |
| 8 | goes on in the executive branch and within | NSA | itself and the intelligence community about wh |
| 9 | judges 16 different times, and so this is not | NSA | running off and doing its own thing. This |
| 10 | every two years, and I think that the | NSA | provided all the relevant information to our o |
| 11 | And the other one is that the | NSA | has both of those missions, and we are |
| 12 | out of my lane. That's not an | NSA | thing. That would be a Department of Justice |
| 13 | conversation, and it impacts, it's not just | NSA | , it's not just the government, it's |

**Table 4**: collocates of "NSA" (Ledgett)

Table 5 below shows the clear difference between Ledgett's perception of the NSA and Snowden's. As the collocations show, Snowden presents the organization as illicitly working with private companies to monitor online communication (1, 3), when not actually illegally intercepting traffic (5, 7), setting in place mechanisms to extend the (illegal) surveillance of American citizens (9-13, 15, 18-20), and so on. Similar analyses could (and in due course must) be carried out on other keywords such as "metadata" and "privacy"; it is only through this close, data-driven examination of the discourse that we can really hope to understand how the debates around cybersecurity (and/or civil liberties, or trust in monitoring of online behaviour) are developing.

| | | | |
|---|---|---|---|
| 1 | America to do its dirty work for the | NSA | . And even though some of these companies did |
| 2 | and open Internet should be. Right. So the | NSA | 's own slides refer to it as direct |
| 3 | direct access. What that means to an actual | NSA | analyst, someone like me who was working as |
| 4 | representatives sitting in a smoky room with the | NSA | palling around and making back-room deals abou |
| 5 | reported as the PRISM story that said the | NSA | broke in to the data center communications bet |

| | | | |
|---|---|---|---|
| 6 | a compelled but hopefully lawful manner with the | NSA | , the NSA isn't satisfied with that |
| 7 | but hopefully lawful manner with the NSA, the | NSA | isn't satisfied with that, and because of |
| 8 | at a copy of "1984" on Amazon.com, the | NSA | can see a record of that, the Russian |
| 9 | , I've got to give credit to the | NSA | for using appropriate names on this. This is |
| 10 | on this. This is one of my favorite | NSA | cryptonyms. Boundless Informant is a program t |
| 11 | tonyms. Boundless Informant is a program that the | NSA | hid from Congress. The NSA was previously aske |
| 12 | program that the NSA hid from Congress. The | NSA | was previously asked by Congress, was there an |
| 13 | already exists. It's already in place. The | NSA | has its own internal data format that tracks |
| 14 | for someone like me who came from the | NSA | and who's seen the actual internal documents, |
| 15 | , that there had been no violations of the | NSA | NSA's rules, when we knew this story was |
| 16 | interesting about this, about the fact that the | NSA | has violated their own rules, their own laws |
| 17 | And she then requested a copy from the | NSA | NSA and received it, but had never seen this |
| 18 | again where we've got to thank the | NSA | for their candor, this is a program named |
| 19 | nfrastructure. They're programs through which the | NSA | intentionally misleads corporate partners. The |
| 20 | 're building in backdoors that not only the | NSA | can exploit, but anyone else who has time |
| 21 | seen in the post-9/11 era, is that the | NSA | has traditionally worn two hats. They've been |
| 22 | wise. The Bullrun and Edgehill-type programs, the | NSA | asked for these authorities back in the 1990s. |
| 23 | you. It's a little bit of a | NSA | problem. When we think about in terms of |

**Table 5**: collocates of "NSA" (Snowden)

This section of my paper has sought to show that CDA and CL can and should be used to develop as full and accurate a picture as possible of a text under examination; this is of course a transferrable model, which can in theory be applied to any area of discourse. My concern in applying this mode of study to *these* texts, in *this* intellectual environment, is to make a very straightforward point, alluded to earlier. Cybersecurity marks a point of intersection between the absolutes and clearly-defined variables of the scientific realm and the fuzzier, irritatingly inconsistent domain of human thoughts and belief. As study of the Snowden affair all-too ably demonstrates, trust is not a given, and

public opinion can be swayed; to date, we see little real sign that the debate sparked by Snowden's disclosures is about to conclude. It may, in fact, only just be beginning.

### 3. *Beyond: Edward Snowden* – Words, Pictures and Image warfare

> [we shouldn't] allow the adversary to have a monopoly of pictures. It's like science versus religion. What do we believe – the pictures or the words? (Jamie Shea, in Mackay, Tatham, and Rowland (2011): 32)

For the modest sum of $99, you can now purchase an action figure of Edward Snowden from www.thatsmyface.com, with a range of outfits and accessories. All profits go to the Freedom of the Press Foundation (https://freedom.press/).

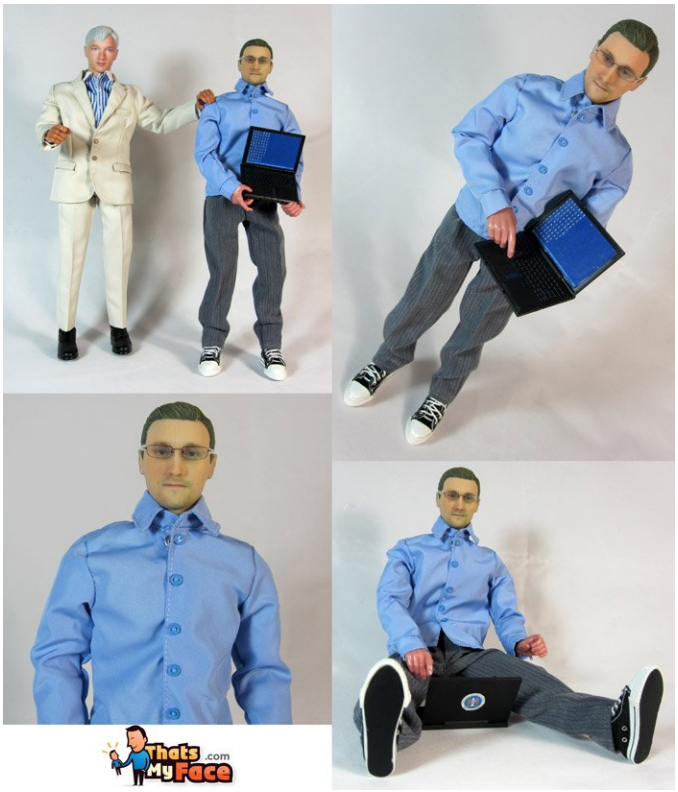


**Figure 1**: Snowden as action figure. Source URL: http://www.thatsmyface.com/images/700x819xedward_snowden_figure_collage_ThatsMyFace_v4_sm.jpg.pagespeed.ic.IN9DDdeUTO.jpg

If that is beyond your reach you can imitate the artist Ai Weiwei, and recreate him in Lego.


**Figure 2**: Ai Weiwei's Lego portrait of Snowden. Source URL: https://naomijwilliams.files.wordpress.com/2015/01/imag0545.jpg

Or construct his escape into exile yourself:

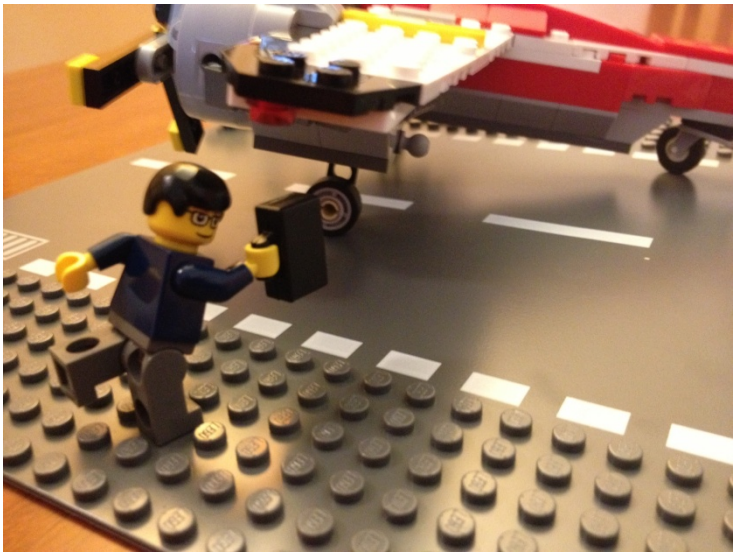

**Figure 3**: Snowden as Lego minifig. Source URL: http://i.imgur.com/DNWQJTn.jpg

Or simply download and print off any number of posters or images which mark the degree to which he has become an icon of popular culture:

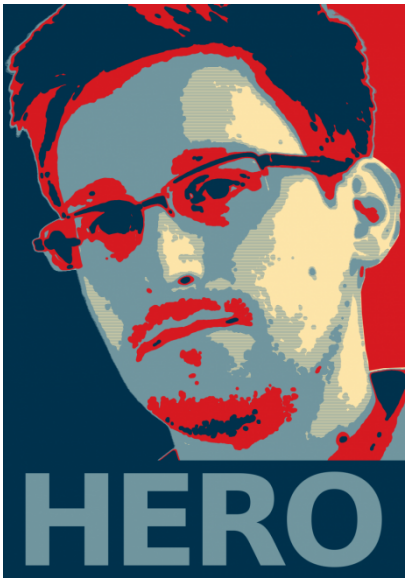


**Figure 4**: Snowden, after Fairey (1). Source URL: http://i.imgur.com/DNWQJTn.jpg http://www.occupy.com/sites/default/files/edward-snowden-hero_v2.png

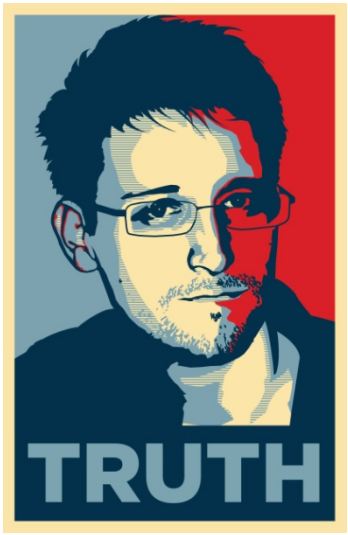


**Figure 5**: Snowden, after Fairey (2). Source URL: https://lawrentianslc.files.wordpress.com/2014/04/eddie-truth.jpg

(note that these last two are appropriations of the style and format of Matthew Fairey's pro-Obama "HOPE" poster)

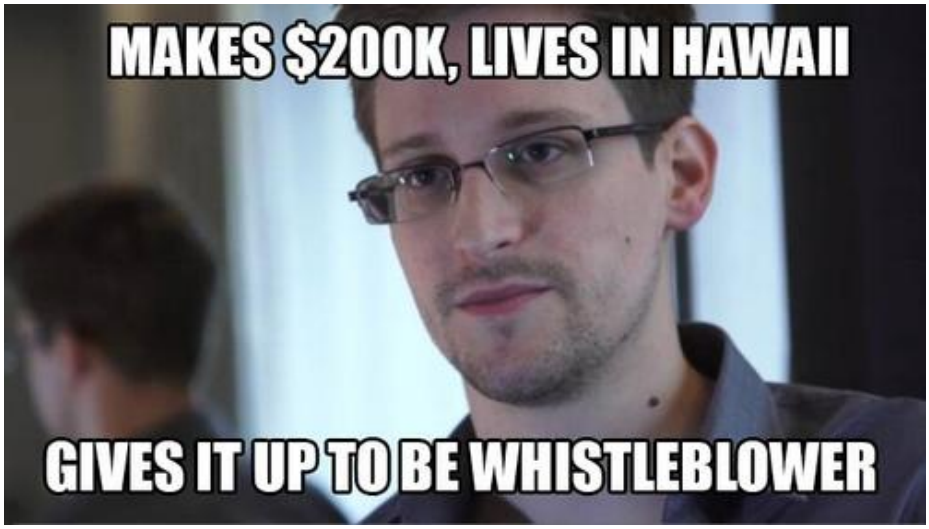


**Figure 6**: Snowden, as internet meme. Source URL: http://www.siliconrrepublic.com/fs/img/tumblr_mo5urrJBOG1qz80pso1_500.jpg

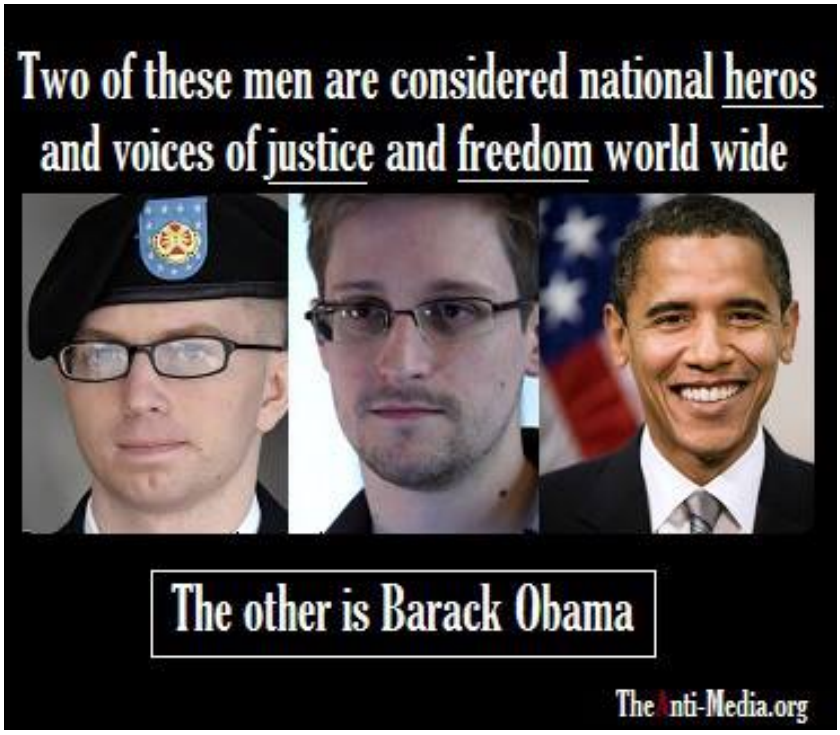


**Figure 7**: Snowden as political weapon. Source URL: http://beforeitsnews.com/contributor/upload/5385/images/998396_252691128189263_625994824_n.jpg

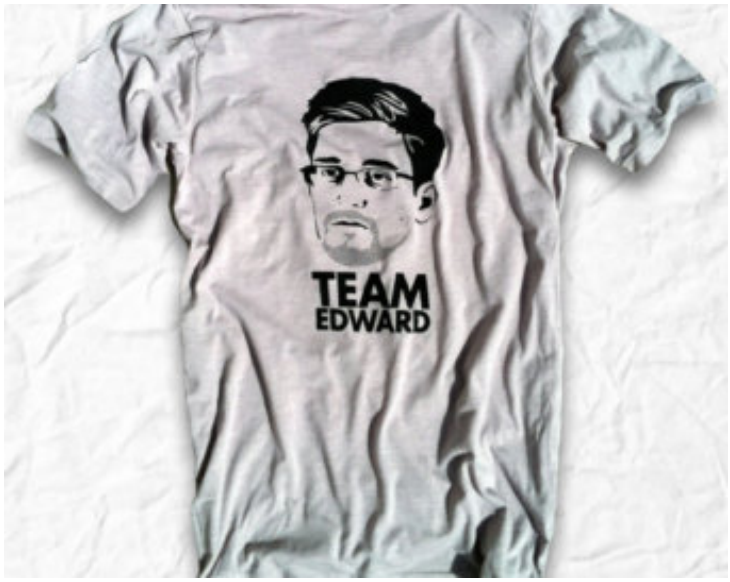


**Figure 8**: Snowden meets Twilight. Source URL: https://img0.etsystatic.com/020/0/5414377/il_340x270.489606310_596f.jpg

(this last image is a particularly pleasing conflation of internet memes)

The point of displaying these images is threefold; firstly, they demonstrate that imagery has a powerful role to play in exerting influence, and the tools to construct what Roger (2013) terms "image munitions" and "counter-munitions" are freely available. Secondly, and crucially, they help to reinforce the concept that this is not a paper about Edward Snowden, but "Edward Snowden", a symbol, a signifier (in Saussurean/Barthesian terms), or the incarnation of an idea, although what that idea may be depends on the person or persons making use of this image. Finally, they act as a bridge between the verbal texts examined in the previous section and the subject under consideration: Edward Snowden, the comic-book hero.

2014 saw the publication of *Beyond: Edward Snowden*, a comic-book retelling of the events in the affair, which presents Snowden as a fundamentally enigmatic figure, who becomes embroiled in a dark world of state surveillance and competing political interests. Written by Valerie d'Orazio and illustrated by Dan Lauer, the text is narrated by an imaginary author, "Virgil T. Hall", who guides us through the labyrinthine complexities of the story; the name "Virgil" seems to be a clear reference to Dante's *Inferno*, where the poet is led through Hell by the Roman poet. D'Orazio has stated directly that she wanted to present the story as a conspiracy narrative, something which has clear implications for issues of government, cybersecurity, and trust:

> One of my big influences for "Beyond" was the old "Big Book Of" series from Paradox Press/Vertigo Comics. Remember those? I must have read "The Big Book Of Conspiracies" until the spine collapsed. Well, I love speculating about current events, I love conspiracy lore, I love the weird and unexplained—and that's what "Beyond" is all about. (D'Orazio (2014))

Rather than presenting a detailed analysis of the way in which *Beyond: Edward Snowden* functions as an example of the multimodal form of the comic strip, what I want to

emphasize here is a more general consideration of what it "means" for his story to be framed within this specific cultural artefact. There is nothing inherently "childish" about the comic strip (such a belief shows a confusion of form and content), as texts such as Speigeman's *Maus* or Bechdel's *Fun Home* show. However, there can be no doubt that, in Western culture at least, the comic strip is primarily a form which presents tales of heroic, godlike individuals, fundamentally *ethical* and *moral* narratives which dramatize quintessential values. One of the best contemporary comics writers, Grant Morrison, sums this up perfectly:

> We live in the stories we tell ourselves. In a secular, scientific rational culture lacking in any convincing spiritual leadership, superhero stories speak loudly and boldly to our greatest fears, deepest longings and highest aspirations […] the best superhero stories deal directly with mythic elements of human experience that we can all relate to, in ways that are imaginative, profound, funny, and provocative. (Morrison (2011): xvii)

Now, *Beyond: Edward Snowden* is *not* a mainstream superhero comic, but it clearly operates within a cultural climate which predisposes us to see the protagonist of a comic as a "hero"; add to this the way in which the work deliberately refers to works of popular culture which present the individual as the unwitting victim of government control and technology-led repression (*The X-Files*, *The Matrix*, *V For Vendetta* are all referenced verbally and/or visually in the text), and we can see a definite process of framing at work. Snowden's actions were *morally* motivated, *technologically* performed, and cause a *political* problem; what we see here, as throughout this paper, is that they have attained a *cultural* significance, which has repercussions far beyond their initial significance. Snowden, in short, has become an image or an icon, and if we are to successfully counter the prevailing belief that "cybersecurity = oppression", we desperately need to develop our own narrative and image-based "counter-munitions".

## 4. Conclusion

What I have sought to do here is to apply a range of analytical approaches and tools to show that the Snowden affair has a cultural impact which can be evaluated through a study of the ways in which image and text transmit much more than simply factual data; this has immense implications for those who wish to influence the current conversation about cybersecurity. We live in a world where popular media (from *Spooks* to *Person of Interest*) present visions of technology as a tool of control, and where the means of instantaneous dissemination of messages on a global scale (and software which allows the production of professional quality texts, images and AV material) are freely available, and used, often by groups and individuals whose beliefs may be radically opposed to our own. My contention is that if we wish to promote trust in our activities, we must learn from the communicative approaches employed by those with whom we most disagree. From Anonymous to ISIS, from Adbusters to Occupy (I imply no moral equivalence between these groups), we can see the highly skilled employment of effective techniques of influence/persuasion/propaganda (delete as applicable) designed to operate in the Information Age. If we are to succeed in engendering trust, we undoubtedly need a message which deserves to be promoted, but it must be presented in a way which makes sense to our audience(s). We need to be studying texts like Boyd and Mitchell's *Beautiful Trouble* (2012) and Reinsborough and Canning's *Re-*

*Imagining Change*, both of which are perfect guides to the techniques used by popular protest movements. We must examine the media artefacts produced by those who are hostile to us, not simply to understand them, but to understand how they promote their causes. We have much to learn from them. Recent press coverage (Sengupta (2015), MacAskill (2015], and Brown (2015)) suggests that such work is beginning in the military domain; it needs to occur in ours. All too often, cybersecurity is about policy and practice; if we are ensure that what we do is trusted, we must also engage with people, and presentation.

**REFERENCES**


Anthony, L. (2014). *AntConc* (version 3.4.3) [Computer program]. Available at http://www.laurenceanthony.net/software/antconc/releases/AntConc343/AntConc.exe (last accessed 1 February 2015).

Ackerman, S. and Rushe, D. (2013). "NSA director: Edward Snowden has caused irreversible damage to US". [online] *The Guardian*. Available at: http://www.theguardian.com/world/2013/jun/23/nsa-director-snowden-hong-kong [Accessed 9 Feb. 2015].

Baker, P., Costas Gabrielatos, Majid Khosravinik, Michał Krzyzanowski, Tony McEnery, and Ruth Wodak. (2008). "A useful methodological synergy? Combining critical discourse analysis and corpus linguistics to examine discourses of refugees and asylum seekers in the UK press". *Discourse & Society* 19, May 2008: 273-306.

Bechdel, A. (2006). *Fun home*. Boston: Houghton Mifflin.

Boyd, A. and Mitchell, D. (2012). *Beautiful trouble*. New York: OR Books.

Brown, L. (2015). "The Army's latest weapon to defeat jihadis? Twitter!". [online] *Mail Online*, 31 January 2015. Available at: http://www.dailymail.co.uk/news/article-2933907/The-Army-s-latest-weapon-defeat-jihadis-Twitter.html [Accessed 3 Feb. 2015].

Chatfield, T. (2009). "The bestselling persuaders". *Prospect Magazine*. [online] 21 October 2009. Prospectmagazine.co.uk. Available at: http://www.prospectmagazine.co.uk/arts-and-books/the-bestselling-persuaders [Accessed 3 Feb. 2015].

*Citizenfour* (2014) Directed by Laura Poitras [Film]. USA: Praxis Films.

*Cool Hand Luke* (1967) Directed by Stuart Rosenberg [Film]. USA: Warner Bros.

De Saussure, F. (1985). *Cours de linguistique générale*. Paris: Fayot.

D'Orazio, V. (2014). “My New Project: Edward Snowden Comic Book Biography”. [Blog] *Valeriedorazio.com*. Available at: http://valeriedorazio.com/post/86234161672/my-new-project-edward-snowden-comic-book [Accessed 2 Feb. 2015].

----., Lauer, D., Oliveira, C. and Beatty, G. (2014). *Beyond: Edward Snowden*. Vancouver, WA.: Bluewater Productions.

Druckman, J.N. (2001). “On the limits of framing effects: Who can frame?”. *Journal of Politics*, 63: 1041-66.

Fairclough, N. (2015). *Language and power*. 3rd edn. Abingdon: Routledge.

Gladwell, M. (2004). “The Ketchup Conundrum - The New Yorker”. [online] *The New Yorker*. 6 September, 2004. Available at: http://www.newyorker.com/magazine/2004/09/06/the-ketchup-conundrum. [Accessed 2 Feb. 2015].

Hirschman, E., Kahneman, D., Slovic, P. and Tversky, A. (1983). “Judgement under Uncertainty: Heuristics and Biases”. *Journal of Marketing Research*, 20(2), p.217.

Lakoff, G. (2004). *Don’t Think of An Elephant!: Know Your Vallues and Frame The Debate*. [e-text]. White River Junction, Vermont: Chelsea Green Publishing. Kindle Edition.

Ledgett, R. (2014**a**). “The NSA responds to Edward Snowden’s TED Talk”. [online] Ted.com. Available at: http://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk [Accessed 2 Feb. 2015].

Ledgett, R. (2014**b**). Transcript of "The NSA responds to Edward Snowden’s TED Talk". [online] Ted.com. Available at: http://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk/transcript?language=en [Accessed 2 Feb. 2015].

Loftus, E. F., & Palmer, J. C. (1974). “Reconstruction of auto-mobile destruction: An example of the interaction between language and memory”. *Journal of Verbal Learning and Verbal Behavior*, 13, 585-589.

MacAskill, E. (2015). “British army creates team of Facebook warriors”. [online] *The Guardian*, 31 January 2015. Available at: http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade [Accessed 3 Feb. 2015].

Mackay, A., Tatham, S. and Rowland, L. (2011). *Behavioural conflict*. Saffron Waldon, Essex, U.K.: Military Studies.

Morrison, G. (2011). *Supergods*. New York: Spiegel & Grau.

----., Phil Jimenez, and Grant Stokes. (1997). *The Invisibles*, vol.2, issue 3, 'Black Science Part Three: Sorted'. New York: Vertigo.

Pratkanis, A. (2007). *The science of social influence*. New York: Psychology Press.

Rapp, C. (2002). *Aristotle's Rhetoric*. [online] Plato.stanford.edu. Available at: http://plato.stanford.edu/entries/aristotle-rhetoric/#purpose [Accessed 2 Feb. 2015].

Reinsborough, P. and Canning, D. (2010). *RE:imagining change*. Oakland, CA: PM Press.

Roger, N. (2013). *Image warfare in the war on terror*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan.

Sengupta, K. (2015). "New British Army unit 'Brigade 77' to use Facebook and Twitter in psychological warfare". [online] *The Independent*, 31 January 2015. Available at: http://www.independent.co.uk/news/uk/home-news/return-of-the-chindits-mod-reveals-cunning-defence-plan-10014608.html [Accessed 3 Feb. 2015].

Snowden, E. (2014**a**). *Here's how we take back the Internet*. [online] Ted.com. May 17 2014. Available at: https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet [Accessed 2 Feb. 2015].

Snowden, E. (2014**b**). "Transcript of "Here's how we take back the Internet"". [online] Ted.com. Available at: https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet/transcript?language=en [Accessed 2 Feb. 2015].

Spiegelman, A. (1986). *Maus*. New York: Pantheon Books.

Ted.com, (2015). *Our organization | About | TED*. [online] Available at: https://www.ted.com/about/our-organization [Accessed 2 Feb. 2015].
[https://www.ted.com/about/our-organization]

*United States Code*. (1947). Title 4, § 8. "Respect for Flag":

Wiener, N. (1988). *The Human Use of Human Beings: Cybernetics and Society.* Boston: Da Capo Press.

*Wired* (2014). September 2014 issue.