Reframing Information: Cyber Warfare Concerns

Abstract: this document was initially and voluntarily prepared as part of an Air Force recruitment inquest. The aim of this short paper is to better frame the concept of *information* both as it is used in *cyber warfare* situations as well as in other scenarios where information is intentionally used by enemy papers to incite violence or destabilize our society. The aim of this paper will be to clarify informational concepts, present simple mathematical formalizations of core concepts, and suggest nascent but actionable solutions.

Adam InTae Gerard **rev. 0.0.10 - 1.16.18**

THIS ARTICLE CONTAINS NO CLASSIFIED, CONTROLLED, NOR CONFIDENTIAL INFORMATION

Reframing Information: Cyber Warfare Concerns

Adam InTae Gerard[1]

0.0. Introduction

This article is humbly and voluntarily submitted per an Air Force recruitment inquest. I make no claim to originality here (though I hope to have stumbled across that inadvertently) as some of the following issues are known and are already being addressed.

However, it is the hope of this brief article to further explicate and better frame those previously-identified concerns to improve remedy outcomes.

0.1. Context

Growing concern over (a) the use of misleading ads by Russia intelligence agencies, (b) the scope of influence that those ads have had on the 2016 election, and (c) the difficulties in identifying both the origins of that information as well as the contents of it has called for a reappraisal of our national digital security policies, posture, and capabilities.

Such concerns have brought to light the ease by which even relatively low-priced informational content can impact and potentially influence a population at enormous scale through ubiquitous digital platforms.

0.2. Objectives

In light of the concerns raised in **section 0.1.**, it is the aim of this short essay to summarize and articulate a few additional concerns regarding the potential use of *information* by *enemy powers*, foreign or domestic, to destabilize the United States in the following ways:

(1) reduce trust between the general populace and its institutions,
(2) increase polarization, division, and radicalization between segments of the populace,
(3) increase the difficulty for the populace and institutions to gain access to good information,
(4) to inflict harm to mental health and well-being,
(5) to gain access to confidential, private, secure, or classified resources/assets,
(6) to inspire fear and violence between segments of the populace and/or institutions.

I believe that (1)-(6) above should be of concern regardless of specific ideological or political preferences (liberal, conservative, socialist, moderate, etc.) given (a) the ability for any ideology or political organization to utilize them and (b) given the potential *collective* harms they pose to an *entire* society when applied by an enemy power to that society.

[1] **Software Engineer**: https://github.com/Thoughtscript/resume/blob/master/current.pdf – **LinkedIn**: https://www.linkedin.com/in/adamintaegerard/ – **Email**: adam.gerard@gmail.com

Specifically, I will attempt to lay out several general approaches (but of course likely not every possible approach) by which enemy powers can (1) disrupt a *good information environment* or (2) otherwise use information to destabilize a society to the point of violence. I will then make several suggestions (which I hope are sufficiently fleshed out enough to be useful) to blunt and remedy those approaches.

I will also attempt to provide three clarificatory frameworks by which to better understand the nature of information warfare. These are simple models that I hope will nevertheless be fruitful for clarifying and quantifying some of the concerns (and therefore be useful in remedying them) upon further refinement by others.

0.3. Caveats and Qualifications

I'm a strong proponent of the view that arm-chair theorizing (purely intuition-based reasoning without recourse to the mathematical or empirical sciences) is limited in its applicability and doubt the assurances of such approaches to make useful predications to desired outcomes.

I take natural science to be a process guided by *at least* empirical observation, providing mechanical causal explanations, and creating reproducible and falsifiable tests.

As such, while the suggestions here are perhaps intuitive and supported by simple mathematical models, I would strongly encourage further investigation and research into them to solidify an approach.

1.0. Definitions and Standards

I will now briefly define *information* and *good information* here noting the historical difficulty in doing so[2]. These are not intended to be "the end all be all" definitions but merely sufficient and compact enough for use in the present discussion. Other papers will elaborate on further considerations as needed and it is my hope that others will further refine these concepts into something much more useful.

1.1. Content, Information, and Good Information

Content: (a) the linguistic meaning of a sentence (a proposition, semantics, or other inferred linguistic meaning such as the *reference* of a *referent*); (b) structure as represented by a formal language (as in physics, maths, logic); (c) structure as represented via any other kind of symbolic representation (i.e. - when natural langauge is used to convey some phenomenon); or (d) the ostensible or stipulated association between one or more things (i.e. - when a pool table is directly pointed to and said to represent a simple kinetic energy example for physics; when we say *this* is *that* when pointing at two things).

Information: information is a discrete unit of *content*.

[2] See Israel and Perry 1990.

Here, the concept of information at play aligns with notions of information as used in the information sciences, communication sciences, linguistics, and philosophy. I explicate the notion to reveal its inherently social and mental character. Information avails itself only when there is a system of *interpretation*. Such interpretations are, for example, captured within the apparatus of *model theory*.[3]

Information is always *information-to-someone* otherwise it "disappears" (speaking metaphorically) into its method of representation (an ant seeing several boulders spelling out the word 'H-E-L-L-O' only see boulders but we as human and English speakers see the word and the boulders – we might even say we see the boulders only as an afterthought so ingrained is the representational edifice of language in our mind and at operation in the brain).[4][5]

Good Information: *good* information[6] is *valuable* information - information that we want to use and often need to use in our reasoning and decision-making for such decisions to have *effective* outcomes.

(1) *Accurate*, factual, trustworthy. E.g. - it must be derived from at least one or more of the following:

- (a) *Factual* - demonstrably true through *deductive* proof, empirical (*inductive* or scientific) test;
- (b) *Well-corroborated* - verified or confirmed through numerous tests, sources, and information;
- (c) *Provably* (*deductively*) true;
- (d) *Intersubjective invariance* - what is common between first-person perspectives[7];
- (e) A correct, *abductive*, inference - what is reasonably the best, non-monotonic, explanation for an observed phenomenon;
- (f) *Highly probable* - per (a and others);
- (g) *Analytically true* – a tautology - per (c and a);

(2) *Safe*. E.g. - the information, content, and representation must be the minimally harmful implementation (within reason).

(3) *Best*. E.g. - the information, content, and representation must be the most useful with

[3] Which are a set of truth-assignments for every well-formed formula in the logic.

[4] As such, it is insensible to say that *information* is a mind-independent objective feature of the world and such nascent *informationalist ontologies* must be careful to weave an understanding of *information* within the considerations just raised.

[5] I believe that *language* is fundamental, allows and gives rise to *information*. I do not see language as intrinsically mind-dependent – rather certain brain-types (human, avian, etc.) are so disposed to speak one or more of them though they, the *languages*, exist independently as a specific class of patterns that are characterized by a *grammar* (such that constituents of the pattern are combined only according to a specified set of combination patterns which are typically described as sets of rules). More fundamental languages are those in which constructions of fundamental linguistic elements like *space* (written language, for example, implicitly requires the use of space and spatial concepts), *directedness*, *mappings*, and *set-theories* can be built.

This is partly what undergirds such motivations as the *Language of Thought* hypothesis though the LOT is not, I believe, a predicate calculus (of whatever order) but rather this more primitive language whose representation consists of *arrows*, *lines*, and *other* diagrammatic symbols each which express those fundamental concepts so constructed in a suitable representation as described above. Such considerations are detailed in a previous paper and enshrined in attempts to rewrite mathematics using *category theory* and *univalent foundations*. See CMU.

From language as understood as an object, we eventually arrive to language as understood as a social system which is to say a language as defined above in use by people to *actually* communicate, describe, order, and express.

[6] I will not speak of *bad* information here nor more precisely the norms governing the acquisition of bad or good information. For the purposes of this paper, we will merely assume that we should endeavor to obtain only good information and better information saying nothing of bad information.

[7] See Cassier 1944, Chester 2012, and Dennett 2007.

respect to specific use-case (within reason). Per (1) above, the best information is derived from satisfying the most number of the listed sources from which the information is derived.

(4) *Consistent*. E.g. - the information is logically consistent within the logical framework in which it is assessed (i.e. - quantum logics reject the law of distributivity).

(5) *Clear*. E.g. - The information is clear, simply put, and unambiguous.

(6) *Improved*. E.g. - The information is corrected in light of error and updated in case of absent information.

1.2. Information Environments

Information Environment: a social setting, (group, situation, context, etc.) within which individuals (people) have and share information with each other.

Good Information Environment: a *desirable information environment* with respect to some set of adjudicating values β(values governing the desirability of the information environment such as freedom, transparency, efficiency, etc.), legal constraints, or some set of goals (free flow of ideas, national security, etc.).

This is an admittedly only a functional definition meaning that I will not argue what The Good or Best information environment here is merely that given certain assumed objectives, legal constraints, or values the most optimal to those is what I shall call a *Good Information Environment*. For the purposes of this paper, I shall then assume that β corresponds to our values, legal constraints, and the goal to see those values flourish within the legal constraints (freedom of expression, national security, Bill of Rights, Constitution, statutory law, common law, maximizing wealth, efficiency, personal safety, happiness, commerce, industry, productivity, knowledge, communication, etc. all within a classically consistent manner which is presupposed by U.S. law[8]).

This is a somewhat imprecise definition and it is my hope that much greater minds than I will help to flesh out this concept in much greater detail.

Conditions for a Good Information Environment: Given the presuppositions made above:

(1) Critical thinking, communication competence, linguistic norms, reasoning skills; and
(2) An appropriate amount of information asymmetry and symmetry accounting for the topology of the information environment (where and how information is distributed); and
(3) How information is transacted (not just the static distribution of information at a given time states).

1.3. Information Asymmetry and Symmetry

[8] That is laws are written with the *intent* that they are logically consistent and when they are not *actually* so, *judicial interpretation* and *review* is then applied to generate a sole source of truth for that legal tension.

Information symmetry captures the notion of information reciprocity (information sharing) and situations where information is had and understood by all parties to a situation. Conversely, *information asymmetry* refers to conditions in which strictly some but not all participants to the situation have some information.

Information asymmetry is not inherently a bad thing. Knowledge has value in circumstances in which it is anti-symmetrical (teaching is the process of making information symmetrical for a price). Classified information is kept secret because it exists in a anti-symmetrical state. Intellectual Property is protected due to NDA's and confidentiality agreements.

I want to take the time to further spell this out below (since formalization usually entails the possibility of building a computational model or simulation).

Let $\prod$ be the total information made available to some individuals $x, y, z, \ldots, n$ in some social setting (group, situation, context, etc.).

Let $'\Omega_{\Phi}$ denote the information Φ available to Ω where $\Phi \subseteq t$ and $\Omega \in \{x, y, z, \ldots, n\}$.

Information Asymmetry: *information asymmetry*[9] is here partially and formally defined by the following relationships:

(1) Ω_k is *weakly information inferior* to Γ_j whenever:

(a) $\{\Omega, \Gamma\} \subseteq \{x, y, z, \ldots, n\}$ and
(b) $j \subseteq \prod$ and $k \subset \prod$ and
(c) Cardinality(k) < Cardinality(j)

(1) Ω_k is *weakly information superior* to Γ_j whenever:

(a) $\{\Omega, \Gamma\} \subseteq \{x, y, z, \ldots, n\}$ and
(b) $j \subseteq \prod$ and $k \subset \prod$ and
(c) Cardinality(j) < Cardinality(k)

(1) *Weak information asymmetry* exists when one individual possesses strictly less information than another.

(2) Ω_k is *information inferior* to Γ_j with respect to a specific $i \in \prod$ whenever:

(a) $\{\Omega, \Gamma\} \subseteq \{x, y, z, \ldots, n\}$ and
(b) $i \in j$ and $i \notin k$ and $j, k \subseteq \prod$

(2) *Information asymmetry* (*simplicater*) exists when one individual possesses specific information that another does not.

(3) Ω_k is *strongly information inferior* to Γ_j whenever:

[9] A concept first explicated by George Akerlof. See Akerlof 1970. In that famous paper, the concept of information asymmetry was introduced to demonstrate what exactly was happening when used car salesmen sell lemons to unwitting customers.

(a) $\{\Omega, \Gamma\} \subseteq \{x, y, z, ..., n\}$ and
(b) $j \subseteq \prod$ and $k \subset \prod$ and $j \cap k = \varnothing$
(c) Cardinality(k) < Cardinality(j)

(3) *Strong information asymmetry* exists when one individual *exclusively* possesses strictly more information that another does not.

Information Symmetry: we may define *information symmetry* per the following:

(1) Ω_k is *information symmetric* to Γ_j whenever with respect to a specific $i \in \prod$ whenever:

(a) $\{\Omega, \Gamma\} \subseteq \{x, y, z, ..., n\}$ and
(b) $i \in j$ and $i \in k$ and $j, k \subseteq \prod$

(2) Ω_k is *strongly information symmetric* to Γ_j whenever:

(a) $\{\Omega, \Gamma\} \subseteq \{x, y, z, ..., n\}$ and
(b) $j = k$ and $j, k \subseteq \prod$

1.4. Information Warfare

Enemy Power: shall here be defined for the purposes of this paper.

(1) A group of one or more violent criminals using information to cause physical harm, incite physical violence, directly or indirectly for some criminal intent;
(2) A nation-state (or any of its governmental or sub-governmental entities) currently engaged in hostile military or cyberwarfare actions against the United States of America (or any of our governmental or sub-governmental entities);
(3) A terrorist organization – domestic or foreign;

Information Warfare: whereby an *enemy power* uses, distributes, destroys, transacts, obfuscates, omits, or withholds information to reduce our *Good Information Environment* to something less than a *Good Information Environment* and/or with the intent to incite or cause physical harm or violence to the United States of America, its citizens, communities, etc. thereby. *Information Warfare* is less costly to wage than a true hot-war.

2.0. Trust Reduction and Enhancement: Trust Adjustment

Warfare since the 1960's has repeatedly demonstrated the effectiveness of *soft power* methods in winning military conflicts. In other words, the allegiance, ideologies, cultural affinities, morale, loyalty, and willingness to fight (rather than the raw military might in terms of bullets, guns, tanks, etc.) of up to an entire population (rather than an assemblage of military units *alone*) plays a significant role and largely determines the outcome of armed conflict in the long-run however successful initial military operations might be.

Soft power leveraged to enhance or maintain trust between elements of composite social organizations plays an essential role in initial state building, maintaining state cohesion (here

meaning the ability for a society to remain intelligibly organized[10]), and to foster both state intra and inter-cooperation. Likewise, information that targets specific elements of society repeatedly and over-time can play an important role in maintaining or improving trust with respect to other composing members of that society.[11]

Conversely, soft power and the use of information to reduce trust can produce the opposite effect whereby trust between members of a society is decreased.[12]

When trust is reduced beyond a minimum threshold, economic transactions can be impaired,

paranoia and social instability come to characterize the normal dispositions increasingly fragmented communities that compose that society, unwillingness to communicate effectively or at all,

general collapse of authority, norm-following and enforcement decays

political efficacy (the perceived efficiency and usefulness of the government) declines.

This should come as no surprise and the empirical evidence clearly supports these observations.

Information modifies beliefs and the acceptance of norms. Through belief modification, information modifies actions. Through the acceptance of norms, information modifies social function.

In fact, if left unchecked it will result in a failed state (ISIS made its initial advances precisely through digital recruitment and mass communication techniques made possible by through gaps in the information environment of the countries in which major territory was lost).

While the recent fiasco with social media being used as a platform for enemy intelligence agencies has received much coverage there has been little in the way of solvency (remedy) or providing counter-reduction methods (ameliorating such detrimental news with positive news). Identifying these maliciously trust-modifying news sources itself has proven difficult.

2.1. Suggested Remedies

News credibility stamp – mandating or recommending that each news article receive a *stamp* of credibility (a logo that would appear somewhere on the media) hosted and maintained by a third-party organization. The credibility stamp would likely be digital and could display:

$$\frac{\text{The total number of accurate articles published by that news outlet this year}}{\div}$$

[10] I do not mean this in a hierarchical way – at least not solely – the way one constructs highways, collects taxes, creates law, builds logistics networks, flies airplanes, etc. must be organized and intelligibly so for any of those social tasks to be possible. That's one of the great achievement of mass production and the factory under Ford and other early industrialists. See Taylor 1911.

[11] The effects of violent media (TV, Games, Movies, etc.) has been studied and published enough that I won't go into it here. Media and information can influence human-behavior to do violent things. The media or information is not usually *the* cause itself – it sometimes is the essential operative motivator, in other cases its not though it may slightly contribute to that outcome (which might have occurred anyway).

12

The total number of articles (retracted, accurate, etc.)

Legitimate news outlets would probably display the stamp to enhance the value of their content and brand. News outlets of all varieties would then, voluntarily or by economic incentive alone, submit their articles to the third-party to verify the accuracy of their content. Depending on the specifics of implementation, the stamp could be entirely consistent with existing free speech rights and regulations (if it were implemented in the manner above, it is).

News outlet origin monitoring – Another way to further substantiate the validity of media content is to track the origin of the content. This kind of media monitoring is only partly existent:

by CHARLES C. W. COOKE *July 4, 2017 4:00 AM*

@CHARLESCWCOOKE

How I fell in love with the United States

EDITOR'S NOTE: *This article originally appeared in the December 31, 2013, issue of* National Review *magazine.*

Figure 1.[13]

We see above that norms surrounding intellectual property, citing, etc. are currently respected by stating where an article first appeared or from where the source of the article at hand was (which may or may not be the actual origin).

Recently, there has been a spate of fake new story retractions by mainstream media outlets[14]. Part of the confusion in those situations stemmed from not knowing where the content *actually* originated from (as opposed to where the content was *attributed* to have come from). And, despite the existence of ad-hoc, voluntary, and localized resources (like https://www.snopes.com/ and http://www.gradethenews.org/) or informally stating where an article originally appeared (per **Figure 1.**) – the actual origin and more importantly, the credibility of the content usually remains opaque. Adding to the *credibility stamp* the origin of the article would be helpful, less time-consuming, and could co-opt existing fact-checking resources. Each article would be assigned a unique hash that would then searchable and linkable (meaning through a relation like a *foreign key*) so that a proper trail of citations could be demonstrably tracked.

This would help consumers to find (more) trustworthy news and media outlets to further validate the quality of the content they publish.

[13] Selected randomly - see http://www.nationalreview.com/article/449156/fourth-of-july-american-exceptionalism-britons-perspective

[14]

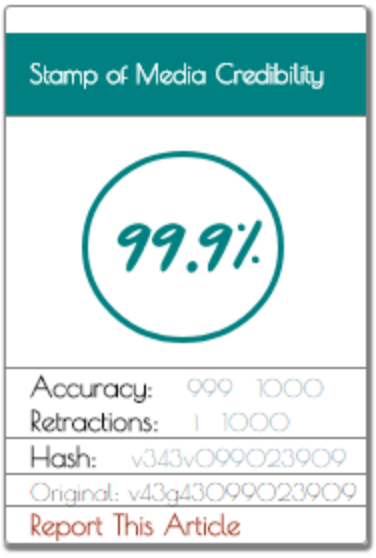

Figure 2.[15]

Trust adjustment – *Mean world syndrome* is a systemic misconception of the world as overly bad, stagnating, declining, falling apart, etc. despite the categorically overwhelming evidence to the opposite[16] (with exceptions for specific regions or individuals). *Mean world syndrome* results from the unique operations of the human brain which privileges news stories about *individuals* over bulk data[17] and selective conditioning (the human brain can only hold about seven items in active memory at a time – consider the millions of news-worthy stories that occur every day).

Requiring news outlets to *balance positive news with negative news* (**not with respect to a specific topic**) by presenting on their landing pages at any given time *a fixed ratio of positive and negative news stories* would go a long way toward altering the incorrect perceptions that people have. To be clear, requiring that of a specific and sole topic (say about a person or a specific issue) would likely be a restriction on free speech. Requiring that a strict balance of the aggregate news stories would likely not be. [18]

I suspect that over time, media outlets will find it in their interest to advertise this as a voluntary feature of their services – particularly as the population becomes better educated and understanding of cognitive psychology and the *hard* neurosciences becomes more prevalent.[19]

[15] Section **12.0.** contains the code to build the example in **Figure 2.**

[16]

[17] Lenin's remark that, "*One* person is a tragedy, a *million* is a statistic" has an empirical basis – interpersonal cognition results from different parts of the brain being activated than purely quantitative or logical thinking. See . This accounts for divergences in moral intuitions in the *Trolley Case*. See .

[18] There are pre-existing constraints on the use of free-speech – when free expression creates dangerous circumstances within the context of specific-kinds of public areas. This same criterion can be applied to the dangerous cognitive distortions that cause mental harm to the entire populace if left unchecked. In these scenarios, no restriction on perspective, view point, or personal expression is made. Rather, restrictions on specific use of words (content) are made (and only temporarily for the duration of that public context – movie, airplane flight, etc.). This is also a fixed ratio not a delimiting minimum or maximum quantity.

[19] Those sciences that are mathematically precise, discover causal explanations and not just correlations, provide mechanical explanations whether *atomistic*, *relational*, *objectual*, *reductive*, *non-reductive*, etc.

A *positive* news story would be uplifting, inspirational, improvement, charity, demonstrate acts of community, kindness, compassion. A *negative* news story would be about a crime, a tragedy, a violation, etc.

3.0. Digital Division and Conquest: Social Fragmentation

Divide et Impera is a military and rulership strategy dating back to at least late antiquity.[20] The challenge for a single ruler over a large population with many factions is thus, "How do I *alone* compel this mass to obey me (and not kill *me*)? How do I maintain my rule over this mass of people when I am a single person?"

Divide and Rule (DR) is just such a strategy - segmenting society, creating artificial divisions or exacerbating existing ones, and atomizing previously united groups into rivalrous subgroups guided by fierce and factitious personalities.

A direct analogy to DR can be found in the concept of *defeat in detail* (DID) whereby a smaller military unit can defeat a much larger one by dividing the larger group into several groups smaller than itself (e.g. - a 300-man unit is attacked by a 100,000-man unit but decisively defeats the 100,000-man unit by only engaging 100 of the 100,0000 at any given time).

Both strategies have been applied by *Enemy Powers*, foreign or domestic, with the intent to project soft power influence, wage *information warfare* on the United States, destabilize perceptions about core institutions, as a continuation of larger asymmetrical warfare ambitions (terrorism, insurgency, etc.), or to indirectly meddle with American political institutions (like puppeteers pulling the strings of a mannequin).[21]

An appropriately symmetrical information environment can be so deformed so that information only exists in diffuse, siloed, pockets. It can also be so deformed that society as a whole fragments and divides (partly on the basis of systematically conditioned and systemically false perceptions of other groups within that society).

In a democracy, the application of such techniques by enemy foreign powers is doubly worrisome. A democracy obtains its legitimacy from the will of the people - by assent and agreement through the process of *mutual* compact - evident in many crucial areas of the political body: deliberation, freedom of speech (which is not merely the act of solipsistic soliloquy but, particularly in tandem with the right to assembly, a dialogue), voting, judicial review, trial by jury, etc.

3.1. Suggested Remedies

[20]

[21]

Internet as a public utility – others have called for the internet to be nationalized and made into a public utility and to not nationalize the internet but nevertheless treat the internet as a public utility.[22] The specifics of these proposals remain mysterious and opaque. The idea behind treating the internet as a public utility is that it creates (more) equal opportunity, is akin to the vehicle highway system (which all benefit from), and to reduce unfair, undesirable, or inefficient information asymmetries in the market.

I want to briefly describe two clarifying remarks to help better situate this debate:

(1) Treat the internet as a public utility serviced by numerous private sector entities.

(2) Treat the information on the internet as a public good but don't treat the internet as a public utility.

On (1), treating the internet as a public utility does not necessitate nationalization. There are a variety of different means by which regulation and public ownership of the internet could be asserted without disturbing the current patchwork of corporations that currently supply the infrastructure for it. Some of these presently exist in various forms (tax deductions, grants, etc.):

(a) *Access* to the internet by means of devices, web-browsers, etc. could be a public service without mandating that the hosting and network infrastructure be.

On (2), treating the information on the internet as a public good not the internet itself.

Intent – intentionality is considered to be a difficult topic within philosophy and natural language parsing but tools now exist that significantly improve on our ability to infer intent from writing.

Intent of the articles is also relevant. Is the purpose of the article to state an opinion (as divisive as it might be)? Or is the article presented to inflame and destabilize?

4.0. Information Asymmetries

[22]

As mentioned in **section 1.3.**, not all *information asymmetries* are undesirable. Classified national security dossiers, intellectual property, and knowledge are desirable kinds or manifestations of *information asymmetry*.

This section, **4.0.**, will explore information asymmetry as it pertains to (1) *anonymity* and (2) *information obstruction*. Neither of these are inherently bad (meaning contrary to a *good information environment*) but both can

4.1. Anonymity

4.2. Information Obstruction

I define information obstruction as an information asymmetry resulting from the willful obfuscation, deliberate misinformation, reduction of quality tools to find *good information* (as defined above)

By "cluttering up" information symmetries so that information becomes lopsided through obfuscation, deliberate misinformation, reduction of quality tools to find information, etc.

4.3. Suggested Remedies

Misinformation reporting, coordinate with public libraries to create a central news database that displays news corresponding to the same item from each of the major competitors.

Some symmetries should be broken. Preventing the dissemination of extremist propaganda (and simultaneously isolating, containing it with counter-arguments and counter-propaganda), children's access to pornography, and elicit selling of drugs or other illegal items are all examples. In those cases, information symmetry is highly detrimental to society.

The main problem with those issues has to do with enforcement specifically with respect to the way the internet and website responsibilities have traditionally been handled. At its core, the internet is a simple set of protocols, devices, and networks that communicate with each other. There's nothing built into the internet at that level to enable any kind of universal filtering. Instead, each site must comply and those that are bad actors, don't.

Another possibility, though draconian, is to curate and maintain fixed search lists. Merely a fixed set of banned URL and IP addresses. This is administered in an ad-hoc fashion through IP blacklisting (which usually just blocks end-users from accessing a site) though various ISP's will maintain additional blacklist and whitelists data sets.

The government need not curate comprehensive lists of URL's as a free-standing government service, it can do so by purchasing website data from multiple sites in order to scrutinize unlawful activity. That site list could be enforced through an API to a distributed database system (perhaps a blockchain) that each search engine would be required to cooperate with (but in this very minimal way).

The way this could be implemented would be open to many lesser or greater kinds of restriction depending on the degree of regulative flexibility.

5.0. Internet Trolls as Agents of Enemy Foreign Powers

Some but not all internet trolls are likely to be (a) fictitious personas used by (b) foreign agents to intimidate, harass, and attack vulnerable and news-getting persons. This has the

The Parrot Principle: most academic research merely parrots or duplicates pre-existing academic research in slightly modified format.

Most research has focused on cyber-bullying as a phenomenon emerging from hostile peers of a victims. Little research has focused on the national security dimensions of cyber-bullying.

Anecdotally, we can see how through such activities the perceived futility, vulnerability, and insecurity of regular citizens (children in particular) could have an enormously morale-reducing impact.

5.1. Suggested Remedies

Incentivize troll reporting – internet trolls harm business experiences, disturb citizens, etc.

There's a clear distinction between trolls and divisive opinions. Trolls insult others (business, person, etc.) – the point of demarcation depends on delivery, language used, and content. Would such a message constitute verbal abuse, harassment if delivered to the person insulted.

6.0. Shell Companies, Botnets, and Security

Many of our country's enemies operate command-style state-based capitalisms. As a result, information warfare is often conducted using elaborate networks of corporations (shell or not) registered or otherwise disguised.

One example is the VPN network Hola.

6.1. Suggested Remedies

Publicly track all security breaches, the companies comprised, the impact on end users, and any company or organization believed to be responsible. While this exists informally (through specific news stories) no such system comprehensively states the security track-record nor the companies involved. In some cases, the companies involved were operating in concert with enemy powers. In other cases, criminal or terrorist organizations directly benefited.

One system that provides a great deal of information but almost purely at the fundraising level is CrunchBase.

7.0. Cognitive Exploit

Meme's can be engineered and constructed (idea architecture and engineering) now... it makes sense to regulate in a minimal way... Dawkins.

7.1. Suggested Remedies

Overlaying (so as not to infringe on free-speech) or requiring of freely spoken speech the following conventions to overcome specific biases that lend themselves to overly negative impressions of specific institutions or people (or at least monetarily incentives reduction of cognitive fallacies in media but also incentivizing reduction of cognitive fallacies in readership from those media-sources – insofar as such cognitive fallacies induce violence):

(a) Stressing that some is not necessarily all.

(c) Specifically warning about what biases are likely to be formed but otherwise letting people form their own opinions.

Reviewing the specific visual and linguistic techniques being deployed in a piece of media. This will become more important as newer and more sophisticated (and experientially comprehensive) kinds of media become prevalent: telepathy (direct brain to brain information sharing, mind-reading (direct brain-reading), holograms, and augmented reality all represent...

8.0. Incendiary Information

If enough about a person is known, it is possible to modify or alter that person's decision-making and actions. In marketing that is quite common – display an ad, get someone to research the ad or buy the item. That's usually quite innocuous and, in fact, usually quite beneficial.

Suppose though that we are considering people on the verge of being violently radicalized – a key tweet, text, or other informational unit can be what pushes someone over the edge. Conversely, a decisively placed piece of information might prevent someone from radicalizing.

To better understand the calculus that would likely be used to influence people in this way, let's review a simple model.

Typed Information:

Type A = {*qq*, *yy*}

Type B = {*uuu*, *www*}

Here, we more formally spell out our concept of an *information environment* using a set of *information types* (each a set of specific pieces of information). Alternatively, we could model this as a domain of information such that types of information are represented as extensions of that domain.

Rational agents (people) are represented are sets of functions mapping *information types* to [0, 1] where [0, 1] represents an interval between two binary, diametrically opposing/opposed, actions or beliefs (representing a state of belief or actionable outcome as a continuum):

Agent_1 = {Type $A \rightarrow .7$, Type $B \rightarrow .3$}

Agent_2 = {Type $A \rightarrow .2$}

Agent_3 = {Type $B \rightarrow .9$}

.

.

.

The set of functions above represents the predicted and/or actual impact of a type of information on that person (agent). We say that these functions are just potential outcomes that are manifested when an instance of the relevant type of information is *actually* received, consumed, or processed by that agent.

This is just a simplified model - in the real-world rational agents (people) deliberate, interact, debate, seek out information to corroborate, etc. These sorts of epistemic and social activities represent a way that incendiary information can be mitigated (insofar as people are open to rational discussion).

Epistemic and social activities also represent a critical component required to maintain a *Good Information Environment*. As such, enemy powers will attempt to systemically undermine the cognitive and intellectual capabilities of a society (schools, universities, mental health, etc.) to steadily reduce an *information environment* to one in which the simple and cold calculus above can be used to incite violence.

When such epistemic and socially systems are sufficiently undermined, an information environment would be reduceable to the simple calculus of information and effect given above.

8.1. Suggested Remedies

Information warfare in this case requires first gathering data on the agents in the environment and then determining how best to reduce the environment to a state where all manifested impacts go to 0 (violence). Here, information asymmetry becomes increasingly valuable...

9.0. Conclusion

This paper has identified several features of information warfare, proposed several operationalized definitions for better address informational concepts, supplied two mathematical models for three inter-related foundations, and offered nascent remedies to four specific kinds of information warfare attacks on those three information foundations.

10.0. Works Cited

Akerlof, George. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism" *The Quarterly Journal of Economics* Vol. 84, No. 3. (Aug., 1970), pp. 488-500.

Awodey, Steve. https://www.cmu.edu/news/stories/archives/2014/april/april28_awodeygrant.html

Cassier, Ernst. "The Concept of Group and the Theory of Perception" *Philosophy and Phenomenological Research* Vol. V, No. 1. (Sept., 1944), pp. 1 -36.

Available here.

Chester, Marvin. "Is symmetry identity?" Arxiv. 2012 pp. 1 – 28.

https://arxiv.org/ftp/arxiv/papers/1202/1202.0292.pdf

Dennett, Daniel. "Heterophenomenology Reconsidered" *Phenomenology and the Cognitive Sciences* Vol. 6, No. 1-2 (March, 2007), pp. 247-270.

Available here.

https://www.pcworld.com/article/2928340/ultra-popular-hola-vpn-extension-sold-your-bandwidth-for-use-in-a-botnet-attack.html

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/TrinidadandTobagoNationalCyberSecurityStategyEnglish.pdf

http://journals.sagepub.com/doi/abs/10.1177/1555412015592473?journalCode=gaca

http://www.cybercrimejournal.com/shaheenhoff.pdf and http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.586.7345&rep=rep1&type=pdf

https://www.politico.com/story/2017/11/01/google-facebook-twitter-russia-meddling-244412

11.0. Author Information

Resume: https://github.com/Thoughtscript/resume/blob/master/current.pdf

LinkedIn: https://www.linkedin.com/in/adamintaegerard/

Email: adam.gerard@gmail.com

12.0. Code Snippets

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="apple-mobile-web-app-capable" content="yes">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Credibility Button</title>
    <meta name='author ' value='Adam InTae Gerard'>

    <!--
    ********************************************************************************
    *                                    STYLES                                    *
    ********************************************************************************
    -->

    <link href="style.css" rel="stylesheet">
</head>

<body>
    <div class="wrapper">
        <div class="buttonWrapper">
            <div class="header underline">
                <h3>Stamp of Media Credibility</h3>
            </div>
            <div class="underline percentWrapper">
                <h5 class="percent">99.9%</h5>
            </div>
            <p>
                <span class="label">Accuracy: </span><span class="num">999</span><span class="num">1000</span>
            </p>
            <p class="underline">
                <span class="label underline">Retractions: </span><span class="retracted">1</span><span class="num">1000</span>
            </p>
            <p class="underline">
                <span class="label">Hash: </span><span class="num">v343v099023909</span>
            </p>
            <p class="underline">
                <a href="https://www.politico.com/story/2017/11/01/google-facebook-twitter-russia-meddling-244412" target="_blank">Original: v43g43099023909</a>
            </p>
            <p>
                <span class="label retracted">Report This Article</span></span>
            </p>
        </div>
    </div>
</body>
</html>
```

Figure 3. - button.html

```css
@import url('https://fonts.googleapis.com/css?family=Nothing+You+Could+Do');
@import url('https://fonts.googleapis.com/css?family=Poiret+One');

html, .wrapper {
    position: absolute;
    min-width: 100%;
    padding: 0;
    min-height: 100%;
    font-family: 'Poiret One', cursive;
    font-size: 11px;
    font-weight: 500;
}

.header {
    background-color: teal;
}

.header > h3 {
    color: #fff;
}

.buttonWrapper {
    position: relative;
    left: 35%;
    top: 250px;
    border: 1px solid gray;
    box-shadow: 1px 2px 1px 1px gray;
    border-radius: 3px;
    max-width: 180px;
}

p {
    margin-top: 1px;
    margin-bottom: 1px;
}

span, a, h3 {
    padding-left: 12px;
    padding-top: 13px;
}

br {
    font-size: 1px;
}

.label {
    font-size: 14px;
    font-weight: 600;
}

.uuid {
    font-size: 12px;
}

.num {

    font-size: 12px;
    color: #1daec0;
}

.retracted {
    color: #a33922;
}

.percentWrapper {
    max-height: 50px;
}

.percent {
    font-family: 'Nothing You Could Do', cursive;
    padding: 15px;
    border: 3px solid teal;
    border-radius: 50%;
    max-height: 65px;
    max-width: 65px;
    position: relative;
    left: 21%;
    color: teal;
    font-size:45px;
    bottom: 58px;
}

.percent:hover {
    border: 3px solid #a33922;
}

a {
    color: #000;
    font-size: 12px;
    text-decoration: none;

}

a:hover {
    color: #a33922;
}

.underline {
    min-width: 100%;
    border-bottom: 1px solid gray;
}
```

Figure 4. - style.css