Influence Operations

by Fred Cohen, Ph.D.

Introduction – cyber war

Cyber war is an ill defined term. It generally may be though of as including any high intensity conflict involving automated systems. In that sense it includes automation as weapons, targets, venues for fighting, and means to ends. In this chapter, influence operations will be the focus.

Cyber-war and influence operations

Sun Tzu said it clearly several thousand years ago in “The Art of War”:[1] “supreme excellence consists in breaking the enemy's resistance without fighting... the skillful leader subdues the enemy's troops without any fighting”. This is the essence of influence operations; anything intended to sway the body politic of any party involved.

Recent events show the enormous impact of influence operations. The dramatic evolution of social media, ranging from bulletin boards, to usenet news groups, to mailing lists, to web logs (blogs), to massive multiplayer online games, business and social affinity group sites, to dating sites, has emerged as a major influence in fomenting mass protests and has been prominently used against police actions, in revolutionary movements, and in support of terrorism.[2] Governments are increasingly seeking to better understand and control social networking environments, and sub-state actors are increasingly using social networking to command and control actions, support recruiting, gain and maintain funding, plan and cary out activities, and for other related purposes.[3] Attempts to provide analysis of social media is outstripped by the innovation of application developers who combine social media with mobile device capabilities to create such things as maps with near-real-time pictures of police and their locations, fed to anyone who wishes to use it.[4] The increasing demand for privacy and security fed by the increasing rate and quality of attacks on networked sites has led to an increasing set of diverse protective measures that seek to conceal and encrypt content, exhanges, and connections.

1 Sun Tzu, “The Art of War”, (Lionel Giles, trans.) May, 1994.
2 Marc Goodman, “Killer apps - The revolution in network terrorism”, Jane’s Intelligence Review, July 2011.
3 F. Cohen, et. al., “Issues in Cyber-Terrorism”, 2000. A DIA sponsored study.
4 For example the iPhone application “Sukey”.

The potential for use and abuse is revolutionary in terms of real-time control over events and the use of feedback from millions of devices to adapt planning to circumstances on the ground. Seeing this, reactions from governments have been sporadic at best, ranging from local transit authorities (i.e., the 2011 shutdown of cellular telephone services in the Bay Area Rapid Transit (BART) system in anticipation of a possible protest),[5] to the shutdown of the Internet in Egypt during their January 2011 revolution.[6] This old-style approach of trying to stop political protest by silencing its messengers looks like a feeble versions of the Soviet Union's last throws, where the start of the revolution was a battle over the main radio and television broadcast station in Moscow.

But unlike Moscow in the late 20th century, today's Internet forms the critical communications infrastructure required to operate financial markets, control power systems, coordinate emergency response, provide logistical and operational support for 95% of US military operations, operate most of the telephony in much of the world, support electronic messaging used for coordinating medical emergency response, paging, tracking of vehicles, surveillance systems, and the list goes on and on. Shutting down such systems, as apparently appealing at it may be at first glance, leads to social havoc and will ultimately destroy any government that attempts it, at least at such a large scale. Even Iran couldn't shut down its Internet during the protests following its 2010 elections.

Prevention and its practical limits

A further problem comes when nuanced shutdowns are attempted. For example, if Twitter® is used to coordinate actions, a simple view that shutting down Twitter® while keeping the rest of the Internet operational would discombobulate the coordination. But this fails because protesters can rapidly move to Facebook®, and from there to LinkedIn®, and from there to World of Warcraft, and from there to wherever they choose to go next. A basic understanding of the Internet concludes that, regardless of what you try to control, any

5 L. Weinstein, “BART, Cell Phones, Lenin, and a Steel Cage”, See: http://lauren.vortex.com/archive/000889.html

6 C. Kanalley, “Egypt's Internet Shut Down, According To Reports ”, The Huffington Post, http://www.huffingtonpost.com/2011/01/27/egypt-internet-goes-down-_n_815156.html 2011-01-27

communications channel can be used, albeit at reduced bandwidth, to communicate any message. This has been well known since the start of information theory.[7] Similarly, trying to lock out some computational method or resource has proven ineffective because any general purpose computation mechanism can be repurposed to perform any other computation, albeit with performance effects.[8] In practice, this is also why firewall systems fail to fully protect internal systems, and this is why technical protections that allow sharing and general purpose function are insufficient to prevent computer viruses from spreading to the transitive closure of information flow.[9]

In addition to the technical limitations in trying to prevent influence operations, there are some serious political issues that go to the heart of free society. The right to free speech asserts, in essence, that in the public square of the Internet, people can say whatever they wish, and others can freely listen to them. Of course this does not extend without limits. Calls for insurrection, slander, crying fire in a public theater that is not in fact on fire, solicitation of murder, and many other similar sorts of things are still illegal, and the question of exactly what speech or non-speech communications are permitted in the commercial space of the Internet are not in the realm of settled law, either in the US or globally.

The interaction of common carrier law with content control has been explored to a limited extent, but Internet Service Providers (ISPs) seem to be in a niche where the law has yet to deeply penetrate. Issues like who can control what aspects of bandwidth and traffic flows on what basis are running into wiretap laws, issues of anonymity, requirements to keep business records, liability for false statements made, use and abuse of technical mechanisms, possession of access keys, and any number of other legal issues. So-called cloud computing is exacerbating search and seizure issues, tracking and tracing, attribution, responsibility for stored content, encryption, and liability for meeting the myriad of

7 C. Shannon, A Mathematical Theory of Communications, Bell Systems Technical Journal. 3, no. 27, (July 1948).

8 A. Turing, On Computable Numbers, with an Application to the Entscheidungsproblem, London Math Soc. Ser 2. Vol 42,Nov 12,1936,230-265.

9 F. Cohen, "Computer Viruses - Theory and Experiments", DOD/NBS 7th Conference on Computer Security, originally appearing in IFIP-sec, 1984.

regulatory regiments associated with privacy, integrity, secrecy, accountability, intellectual property rights, and use control. Safe harbor laws violate privacy regulations, outsourcing and offshoring bring into doubt the insider vs. outsider access control issues, and the entire basis for security associated with loyalty is becoming muddied along with the increased interdependency of components, composites, systems, networks, infrastructures, and support systems on an ever-increasing set of disparate global actors.

To move forward quickly in the information technology arena, society has sacrificed much of what made it work and the basis for how it worked. This is not a good or bad thing – it is simply a fact. A change in culture is underway, and the days of walking to the library to look something up over hours to days is no longer. Now, we are overwhelmed with information of a wide range of quality, there is little editorial review for much of the content, and people see what they see and believe what they believe.

The anarchy of the early Internet is slowly yielding to power and influence in the form of financial resources that allow more or less visibility, presence in search engines, advertisement, linkage with broadcast media to create and support fads, and all of the other sorts of media control and influence tactics that have long held sway. The cost is lower, the influence broader, the customization of market influences far more advanced, the characterization of individuals and messaging directly to them more stark, and the potential for use and abuse greater than it has ever been before.

The underground of World War II that struggled against Germany would be hard pressed to exist in the World of today. Increased surveillance technology, better analysis and coordination, the ability to listen to every call, read every message, take over the computers that operate the encryption mechanisms to surreptitiously get the keys and read/forge messages, and all of the other technical exploits that are becoming more and more a part of the technology over time, provide the potential that the malicious corporation, government, transnational, or sub-state actor could destroy such an underground or turn it for other use.

Prevention is critical to limiting influence operations, but our society is in a rush to move forward, and the movement brings with it the

limitations of current technology. Prevention is failing and becoming weaker every day. Unless we slow progress in building the very machine that we are using to revolutionize the World, we will not be able to prevent any of these sorts of things from happening.

Deterrence and its limits

Given the inability to technically prevent influence operations in the Internet without destroying the society that the Internet supports, classic security alternatives include deterrence, detection and reaction, and adaptation. Deterrence is an influence operation.

The goal of deterrence is to cause people to not do things that they might otherwise do, by convincing them not to. Fear, uncertainty, and doubt (FUD) is one approach, and this is reflected in part of the "security theater"[10] of modern airports. The Transportation Safety Authority (TSA) decides, based on unpublished criteria, whether to look at you naked, touch you all over your body, or use electromagnets to detect what you are carrying. You have to take off your belt and shoes, remove personal items, and subject them to seemingly arbitrary search with a technology that does who knows what. They may swipe you with a special piece of paper and put it in a machine that beeps if you have traces of some unknown combination of chemicals that tell them if you used a gun lately, even though that act is legal. They ask you personal questions about your travel plans, and if your name is similar to that of someone else they suspect for unknown reasons, you can't get a boarding pass like everyone else.

Fear of the unknown, certain knowledge that you will get caught, and yet testing has repeatedly shown that the actual controls do not work all that well. I have accidentally forgotten to remove a knife from my pocket before flying and had it pass through security in both directions. And in first class on an international flight in 2011, the flight attendant gave me a metal knife to eat my meal with that would not be allowed through security on my person. So the fear is certainly provided, but the reality of the system is far less effective. Arguably, the risks associated with skyjacking for military-like effects were mitigated on 2001-09-11 when Flight 52 was crashed

10 B. Schneier, "Beyond Fear: Thinking Sensibly About Security in an Uncertain World.", Springer, May 4, 2003.

in Pennsylvania in a passenger revolt against the terrorists. No further action was required to prevent the higher consequences, and anyone seeking to take control of an aircraft after that time has been rebuffed by other passengers.

“The only thing we have to fear is fear itself”,[11] and that fear is what is often used to manipulate opinion and influence people. Fear of prosecution prevents some number of people from committing crime, but fear also keeps some people from venturing out of their house. Sewing fear in a population brings with it a withdrawal from markets, distrust of others, xenophobia, mistrust, and all of the things that go with them. From the Salem Witch Trials to the McCarthy Era, fear, rational or not, has been exaggerated to the detriment of free society. When societies use fear to deter crime, they usually foster insurrection, underground economies, and an internal struggle. But ideally, for a society to grow and prosper, we want the opposite sets of behaviors. That's likely part of why free societies have historically done better than enslaved or suppressed ones.

But there are deterrent approaches other than fear. For example, social norms and educational approaches that teach children about the good and bad nature of human behavior helps to reduce undesired behaviors. Don't speak to strangers has an Internet analogy, and yet the free and easy social interactions fostered by Internet technology discourages such levels of filtering based on appearance, accent, race, ethnicity, or other similar social clues that have classically driven liking and helped to drive resulting comfort with message.[12,13] These clues have been replaced by other social clues, such as expressions, reputation, language usage, familiarity with special symbol use and annotations, and other c001 stuff like that ;). And of course these social clues are easily forged by those who use successfully deception in the Internet environment, just as they are forged by confidence experts in the physical environment.

11 F. D. Roosevelt, during his first inaugural address in 1933.
12 R. Cialdini, “InfluenceInfluence: Science and Practice", Allyn and Bacon, Boston, 2001.
13 Bob Fellows, "Easily Fooled", Mind Matters, PO Box 16557, Minneapolis, MN 55416, 2000

As a society, we have yet to evolve the social norms for Internet behaviors, and the social norms of different forums form online communities that, from a legal standpoint, may have the same sorts of community standards rights and limitations as physical communities. If one physical location views pornography in one way and other in another way, will the online analogy – the informational community – have a similar latitude in enforcing community standards? These are unsettled influence issues in the information arena, and part of the challenge of forming a more perfect union in the Internet era. The battle for the hearts and minds of future generations lies in their online communities, and these communities are being used to influence our children and our societies.

Generally, more honest communications are viewed as beneficial to a free society. In the marketplace of ideas, survival of the fittest rules the day, as long as ideas have the opportunity to grow and prosper. The notion of the meme[14] defines the unit of reproduction in the marketplace of ideas. Memes, like different notions of God, popular videos, new word usages, and popular music, spread and reproduce both within and between people, and spread like a disease in the fertile field of human discourse. The Internet is a place where memes are spread further and faster than ideas were ever able to spread in human history before. Our social and political structures are not built to handle ideas that spread so quickly and compete so openly across the globe.

Our ability to cope with deception in the Internet is poor at best. We cannot readily attribute memes to people, because in the Internet, identities are pseudonyms for influence actors we may never have met. Individuals may have multiple identities and spread memes for their own purposes ignoring any need for truth. The problem lies largely in trust relationships, which have historically been based on repeated interactions within relatively small groups of people who must live where they are. Trust building interactions and reputations based on long histories don't exist in the same way in the Internet. There is little to lose for malicious actors. A small informational investment in building up trust over time is used for advantage in a

14 R. Dawkins, “The Selfish Gene” (2 ed.), Oxford University Press, p. 192, ISBN 0-19-286092-5, 1989.

one-time deception. And these interactions can be bought and sold in the commercial market. Third party participants are paid small fees to build trust with time in personae offered for sale to the highest bidder. You don't have to lie in the bed you made for yourself, someone else made it for you, and nobody needs to lie there after it is exploited for advantage. Without stronger attribution, there is no deterrence for these sorts of activities, and attribution also implies taking responsibility for your own actions over time, and an end to anonymity.

Without attribution, deterrence is unlikely to be effective regardless of the methodology used, because there is no punishment for failure to comply. As long as this remains the case, deterrence will at best be an unstable situation in which anyone who breaks the social contract with due care is rewarded instead of punished. If recent history is an indicator, the call for anonymity in support of freedom from oppressive governments will continue to prevent attribution from being effective writ large. But attribution technology is advancing in the forensics arena, and there are many examples of successful attribution despite the attempts to use deception and anonymity.[15]

Political struggles between freedom and justice lead to battles over anonymity and attribution. But from a purely technical standpoint, there is little to support the many claims in the media of technical attribution. Using authentication for attribution is problematic in most of the Internet space because of the ease of theft of most authenticators and the common practice of doing so. Keystroke analysis and similar authentication methods[16] have proven problematic for other than small populations of known individuals in situations where detailed information is constantly available.[17,18]

15 F. Cohen, “Digital Forensic Evidence Examination”, ASP Press, 2009-2012, Chapter 7. ISBN # 1-878109-47-2

16 Gaines, R.S., et al. 1980. Authentication by keystroke timing: Some preliminary results. Rand. Report R-256-NSF. Rand Corporation. Available at http://www.rand.org/pubs/reports/R2526/.

17 M. Villani, et. al. Sung-Hyuk Cha, "Keystroke Biometric Recognition Studies on Long-Text Input under Ideal and Application-Oriented Conditions", School of CSIS, Pace University, Pleasantville, New York, 10570, 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW’06).

For authentication, error rates are summarized here for different methods[18,19]:

Retina	$1/10^7$	Iris	1/131,000
Fingerprint	1/500	Hand Geometry	1/500
Signature	1/50	Voice	1/50
Face	No data	Vascular Patterns	No data

Stylometrics have been suggested for differentiating between small numbers of individuals.[20] N-gram analysis and other sorts of statistical methods have proven ineffective as well. Unigrams (1-grams), bigrams (2-grams), and trigrams (3-grams) are most commonly used, but this can be expanded to n-grams in the general case. Fisher's exact test (both left sided and right sided), log-likelihood ratio, mutual information, point-wise mutual information, odds ratio, phi coefficient, T-score, Pearson's chi-squared test, and any number of other methods from standard statistical analyses. 3-grams and higher order sequences have also been examined with similar statistical methods, including without limit, N-gram largest token size of value, hidden Markov models, morphemes and phonemes, gender identification, authorship attribution, bag-of-word techniques, and non bag-of-word similarity techniques have also been tried.[21]

In one study, simple deceptions based on statistical word usage were tested by comparative analysis with attribution methods histogram distance, Manhattan distance, cosine distance, KS distance, cross-entropy, Kullback-Leibler distance, LDA, Gaussian SVM, and Naïve Bayes. These were tested against sample set generated from words, 2-3 letter words, 3-4 letter words, word bi-grams, word tri-grams, word stems, parts of speech(POS), word

18 B. Rao, "Continuous Keystroke Biometric System", Media Arts and Technology, September 2005, A University of California, Santa Barbara for partial requirements of Masters of Science in Media Arts and Technology

19 A. Guven and I. Sogukpinar, "Understanding users' keystroke patterns for computer access security", Computers & Security, Volume 22, Issue 8, December 2003, Pages 695-706.

20 C. Chaski, "Who's At The Keyboard? Authorship Attribution in Digital Evidence Investigations", International Journal of Digital Evidence, V4#1, 2005.

21 Survey / Analysis of Levels I, II, and III Attack Attribution Techniques", available at: http://www.cs3-inc.com/arda-survey.pdf

lengths, syllables per word, characters, character bi-grams, character tri-grams, binned frequencies, binned reaction times, and Mosteller-Wallace function words. The sample set had 15 authors with 5,000 words from each, 500 involving imitation and 500 involving obfuscation. Results were indifferentiable from random guessing.[22]

In summary, attribution is ineffective today for use in Internet-scale environments, and many techniques promoted in the media fail to meet the laugh test in terms of actual use in defensive information operations. Deterrence without attribution won't likely work.

Detect and react

If we cannot effectively deter or prevent influence operations without giving up the very freedoms that form the basis of our society, perhaps we can detect and react. Unfortunately, the present technology for detection is poor in that it can be and is regularly defeated by attackers of moderate skill levels. Deception to defeat attribution is a good example of where current deception methods easily defeat current attributions methods.[23] This is likely to remain so for quite some time because of fundamental difficulties associated with undecidability.[24] As was shown in 1986, detection of computer viruses is, in general, undecidable.[25] Similar proofs and demonstrations have shown the same to be true of computer worms, Trojan horses, and a wide range of other technical attacks.

For human influence, of course, this is a different issue. But there are good reasons to believe that the same limitations will apply for human behaviors as computer behaviors, among them, because the models used for computers and computation are based on models of how humans calculate things. Research on human

22 P. Juola and D. Vescovi, “Stylometric Approaches to Author Obfuscation: An Empirical Study”, IFIP TC11.9 Digital Forensics Conference, Orlando, FL 2011-01-31-2011-02-02

23 P. Juola and D. Vescovi, “Stylometric Approaches to Author Obfuscation: An Empirical Study”, IFIP TC11.9 Digital Forensics Conference, Orlando, FL 2011-01-31-2011-02-02

24 A. Turing, On Computable Numbers, with an Application to the Entscheidungsproblem, London Math Soc. Ser 2. Vol 42,Nov 12,1936,230-265.

25 F. Cohen, “Computer Viruses”, Dissertation, University of Southern California, 1986.

influence has been undertaken in the fields of psychology and sociology for many years and excellent summaries of the work in these areas is available.[26,27,28,29,30] It seems clear that there are many well understood ways of influencing behaviors and that these methods are well tested and widely used in marketing, politics, frauds, military operations, and elsewhere.

Detection of influence is in its infancy with almost no current research results worthy of serious consideration. While offensive influence operations are in widespread use and have been for a long time, detection of influence operations are typically the results of investigative reporting or in-depth investigation, and are usually reported long after the effects are felt. For example, when Ronald Reagan announced that the discotheque bombing in Germany the 1980s that killed scores of US service men was the work of one country, it was less than a year later that it was determined that this was not true and announced in the media – and yet the majority of the public questioned about it 20 years later remained misinformed.

In order for detection and reaction to be effective, they have to be sufficiently quick and with sufficient forcefulness to overshadow the memory of the events in near-real time. The human mind tends to remember the first and last impressions best and those in an aroused state more than those without the excited state. By creating a sense of crisis and providing false facts that are spread in the media, even orders of magnitude more information countering the deception on a factual basis and with similar authority tend to fail to undo the false impressions left behind.

There are known cognitive mechanisms and limits associated with these phenomena, such as the desire not to rethink, the effect of ordering on memory, limits of how many things can be considered

26 Bob Fellows, "Easily Fooled", Mind Matters, PO Box 16557, Minneapolis, MN 55416, 2000

27 Charles K. West, "The Social and Psychological Distortion of Information", Nelson-Hall, Chicago, 1981.

28 Robert B. Cialdini, "Influence: Science and Practice", Allyn and Bacon, Boston, 2001.

29 Chester R. Karrass, "The Negotiating Game", Thomas A. Crowell, New York, 1970.

30 Charles Handy, "Understanding Organizations", Oxford University Press, NY, 1993.

at one time, the difference in affect associated with increases in what you don't have versus decreases in what you do have, and so forth. These have been documented in the literature, summarized in a framework,[31] and implemented to a limited extent in software systems such as Influence[32,33] and Decider.[34] But this level of understanding and tool implementation falls far short of a systematic and timely approach to detecting and reacting to influence strategies.

Adaptation

Of course we must either adapt to the changes in the social fabric brought about by the Internet or adapt the Internet to meet the needs of the desired future social fabric.

The notion of social engineering takes on new meanings when it is the engineering by government of the social fabric. Social engineering in the computer security context is typically something done by an attacker against a defender to try to gain access or information through deception. Cognitive errors are exploited in defender systems (including people, organizations, technology, and processes) or components for advantage. But seeking to engineer the social fabric is a far more complex issue and one that is often viewed as propagandistic. On the other hand, government at its heart is social engineering. Even a government that is strictly responsive to the “will of the people”, ends up enforcing the will of the people on those who differ beyond some bounds. Regulations, laws, taxation, providing for the common defense, all involve some level of intentional manipulation of the social fabric.

Societies around the World are adapting to the changing social fabric of the Internet, and this is bringing about dramatic change. The “Arab Spring” of 2011 produced enormous social changes in the nation states of the Middle East where rapid communications

31 F. Cohen, “A Framework for Deception”, (chapter in National Security Issues in Science, Law, and Technology), Thomas A. Johnson, Ed. Taylor & Francis, 2007.

32 F. Cohen, “Influence”, © 2005-11, Fred Cohen & Associates.

33 F. Cohen, “Method and/or System for Providing and/or Analyzing Influence Strategies“, US Patent Pending

34 F. Cohen, “Method and/or System for Providing and/or Analyzing and/or Presenting Decision Strategies“, 60957455 (Patent pending)

and information availability helped to foster and support revolution after revolution. Governments like China are constantly dealing with the challenges of supporting the Internet revolution and the transformation of their society while trying to suppress expressions of dissidents against the government and its leaders.

Adaptation happens at all levels, and the result of adaptation is not limited to enterprises, governments, or groups. Individuals adapt to the changing mechanisms of the Internet as widespread consumer adoption of cloud computing and social networking leads to new styles of interaction, work, and play. A dramatic movement away from the notions of privacy and individualism is taking place with the increasing use of shared services like Google, that are increasingly becoming central to the day-to-day lives of hundreds of millions of people worldwide. This is bottom-up global adaptation of human interaction, communication, cooperation, and competition.

As an influence operation, the notions of hierarchical control over human activities that were seminal to understanding, control, and management of the people of societies and the human world seems to be disappearing altogether. While companies like Google, Microsoft, and Apple are leading this revolutionary change with their technology and service offerings, there are an enormous number of competitors in the space that could do as well or better from a technical standpoint. It is their ability to manage the perception issues that leads to their dominance, and this dominance may not continue if compatibility across all platforms becomes increasingly ubiquitous. What is currently a bottom-up sea change facilitated by limited competition among hierarchical companies may turn into a global marketplace of ideas coordinated by a global marketplace of services and products that interact and interoperate but in which survival is completely dominated by popularity. In other words, the only basis for differentiation is perception, which is produced as a result of influence. The influence operations create the services and support structures that are used to drive further influences.

In other words, adaptation to influence operations drives and is driven by further influence operations. The human discourse is an adaption to memes by memes through memes. Psychology drives and is driven by influence operations leading to a highly uncertain and enormously broad spectrum of futures over shorter time scales.

Influence Operations

Stability of society, thought processes, ideas, influences, and the human internal and external discourse are all subject to different control conditions than have existed throughout human history.

History has shown that this sort of uncertainty ultimately produces a human response that seeks stability. In the past this has been in the form of religion or a charismatic leader, leading to one form or another of hierarchy. While many in the intellectual community may hope for the adoption of a humanistic or scientific adaptation, history does not support this outcome.

For the society wishing to avoid these outcomes, adaptation may take the form of learning how to detect influence operations of all sorts and mitigate those deemed to be harmful to society by exerting positive controls (i.e., using influence tactics) over social influence. Anarchy and government controlled social influence may both be countered or overwhelmed by corporate, individual, or other group influence. Counting these influence operations may be done through regulatory or other intervention. Thus we have a potential balance or imbalance of influence depending on the forces at play and how they interact with each other.

Today, adaptation in the commercial space has taken forms ranging from funding of political action committees (in the US) using money to influence which candidates survive the political process and have a chance to get elected; to advertising giants who are forming markets in real-time provisioning of advertisements to Web sites based on psychological factors identified in behavioral sequences of potential customers.

As the study of human behavior increasingly dominates efforts to sell over the Internet, technology supporting behavioral influence tactics is starting to dominate other approaches to winning in the market. Studies by advertisers show specific behavioral sequences observed prior to specific purchase types, and these sequences are observed in real-time by participants in these markets to determine the price they are willing to offer for the instantaneous advertising response placed on each Web site visited. Response times of a few milliseconds are required in these markets and prices ranging up to several dollars per image shown are being paid today for the advertisements just before buying decisions are made.

Individuals typically expand influence either through the political process, sports, media, religion, or other sources that may be understood as fame in all of its forms. They form groups that may also use these methods, and to the extent that the groups gain the ability to influence, they choose who and what they influence. Thus a constant marketplace of ideas and influences are present in human discourse, and dominance in this marketplace leads to dominance across other markets as the overarching activities of human societies and the individuals that compose and comprise them trend toward the activities supporting the ideas influence puts into that market.

Ideas that succeed must, in the end, provide some set of perceived benefits to some set of people in order to keep then engaged over alternatives that are always present and essentially impossible to eliminate. In the current and emerging information environment, the number and diversity of such ideas is so large that cohesion seems to exist only for short periods of time over limited portions of the space. Unlike our ancestors who had limited information and could be readily controlled through its use, today, the sheer quantity and open capacity to produce differing views makes such direct control infeasible. But this does not have to stay this way indefinitely. Over time, it seems likely that some relatively small number of groups in each of a range of areas of discourse will gain an overwhelming support of the public and their constituents surrounding some set of issues, ideas, and views, and that society will cohere to these as centers of discourse and opinion. This is because of the human tendency to not want to think or rethink and the seeming pack mentality.

And of course, if and as stability appears, the human desire for change, power, individualism, or some other set of internal and external factors may ultimately shake that stability, producing less stable states for a time, perhaps driving chaos into the system, unless and until stability again appears. Nobody today can realistically estimate the ultimate direction of stability and change, if in fact there is such a thing. But it seems clear that we will go through a great number of these cycles before we reach an ultimate in evolution of influence. And it also seems clear that in the interim, the war for influence and the power it brings will be with us.

The weapons of the influence war

War always involves weapons, whether they are the methods used by the individuals or the mass weapons produced with economy of scale. The previous ages of humanity have produced weapons that build on the technologies of the day, and the information technology revolution has only started to bring about the revolution in information weapons.

Information weapons predated people. Communications used to influence conflict ranged from the posturing and displays through signals used to cooperate over time and space. Human persuasion and well defined methods underlying it have existed for thousands of years, and the methods of deception and influence discussed earlier have, over time, yielded to scientific inquiry to produce the current views of the social sciences, predominantly sociology and psychology.

As people explore the physiology of the brain with better and more precise tools, we are finding physiological links to psychological and sociological phenomena. The day may come when we can map brain activity into the methods of influence, perhaps even directly producing signals to effect changes in brain activity with resulting behavioral effects. While this technology would have to be applied en masse to have comprehensive effect, application to key individuals would likely be effective at gaining and maintaining control over an extended period, and with that control, further actions might be used to gain further control.

These methods were explored in efforts like MKULTRA,[35] a CIA operation that, according to The Senate Select Committee on Intelligence hearings of August 3, 1977 and subsequent document disclosures, was an effort to explore and exploit mind control. This included such things as sound frequencies that make people fearful, sleepy, uncomfortable, or sexually aroused; results on hypnosis, truth drugs, psychic powers, and subliminal persuasion; LSD-related and other drug experiments on unwitting subjects; the CIA's "manual on trickery"; and so forth.[36]

35 See: http://all.net/journal/deception/MKULTRA/index.html

36 Much of this discussion is extracted from F. Cohen, “Frauds, Spies, and Lies, and How to Defeat Them”, ASP Press, 2005.

One 1955 MKULTRA document gives an indication of the size and range of the effort; the memo refers to the study of an assortment of mind-altering substances which would (and I quote):[37]

- promote illogical thinking and impulsiveness to the point where the recipient would be discredited in public,
- increase the efficiency of mentation and perception,
- prevent or counteract the intoxicating effect of alcohol,
- promote the intoxicating effect of alcohol,
- produce the signs and symptoms of recognized diseases in a reversible way so that they may be used for malingering, etc.,
- render the indication of hypnosis easier or otherwise enhance its usefulness
- enhance the ability of individuals to withstand privation, torture and coercion during interrogation and so-called “brainwashing”,
- produce amnesia for events preceding and during their use,
- produce shock and confusion over extended periods of time and capable of surreptitious use,
- produce physical disablement such as paralysis of the legs, acute anemia, etc.,
- produce 'pure' euphoria with no subsequent let-down,
- alter personality structure in such a way that the tendency of the recipient to become dependent upon another person is enhanced,
- cause mental confusion of such a type that the individual under its influence will find it difficult to maintain a fabrication under questioning,
- lower the ambition and general working efficiency of men when administered in undetectable amounts, and
- promote weakness or distortion of the eyesight or hearing faculties, preferably without permanent effects.

37 Details are provided under the “MKULTRA Documents” link at the previously cited Web site.

Of course defense against these methods is also at issue. A good summary of some of the pre-1990 results on psychological aspects of self-deception is provided in Heuer's CIA book on the psychology of intelligence analysis.[38] Several other papers on deception detection have been written and substantially summarized in Vrij's book on the subject.[39] A broader range of approaches to countering deceptions suggests that countering deception largely depends on the ability to apply the scientific method to the issues at hand.[40]

Influence weapons are not limited to direct informational attack methodologies. A physical approach like blowing up a building, crashing a plane into a football stadium during a game, or shooting shoppers during the peak of the holiday shopping season has a substantial influence on behaviors. Sustained efforts demonstrating the ability to perform ongoing attacks has a substantial influence on the viewpoint of the targeted population and those looking on from other perspectives. The influence conflict in the battle of Britain was an astonishing example of the will of a people and the influence of their society and its structures in defeating a seemingly unstoppable and endless battering affected in the physical and mental domain by Germany. And yet the bravery shown by the leaders and people of London managed somehow to overcome.

This helps to demonstrate the fact that influence weapons are not all offensive in nature. Defensive weapons of influence include such things as awareness posters (e.g., “loose lips sink ships”), public statements (e.g., “the only thing we have to fear is fear itself”), and obvious physical security (e.g., security theater). The level of fear subsides and national pride arises when enemy leaders are killed, and the clear definition and depersonalization of enemies is an influence tactic that makes killing and, ultimately physical war itself, acceptable. Of course defense is not limited to fear reduction or removal of moral barriers to killing. It goes across the entire spectrum of human discourse, just as the offense does. Indeed, they are indiscernible from the technical standpoint. It's a matter of

38 Heuer, "Psychology of Intelligence Analysis", History Staff Center for the Study of Intelligence Central Intelligence Agency 1999.

39 Vrij, "Detecting Lies and Deceit", Wiley, New York, NY, 2000.

40 F. Cohen, “Frauds, Spies, and Lies, and How to Defeat Them”, ASP Press, 2005.

perspective whether you are attacking or defending a particular point of view or mindset.

Time is of the essence

The problem in applying the scientific method to influence is that is takes a lot of time, and persuasion takes far less time. By the time the facts are checked and reality discerned, the influence has already taken place, and undoing it is often infeasible. This is because of the desire not to rethink, the effect of first impressions, and so forth, as discussed earlier and details in depth in the referenced material. The strategy often adopted is to counter any “rush to judgment” with appropriate persuasion indicating the need to study the issue further, indicating that there are early indicators that this is not true, and so forth. But this approach is also problematic, and the resulting discourse is a political discussion.

Today's media is highly intolerant of well thought out discussion, considered or nuanced positions, and anything that might take more time than the ability to deliver content. The Internet and 24-hour news and media has produced a flood of wrong information that comes quickly and is poorly checked, largely because it is a race to get information out sooner in order to get more readers and thus sell more advertising. Newspapers, which typically have had a more thoughtful editorial approach, presumably because they often have a few hours to make judgments before going to press, are falling by the wayside, and their online equivalents have not adjusted to the editorial needs of real-time news.

The net effect of the tradeoff between better, faster, and cheaper is that better loses in terms of the quality of information. Editorial judgment is largely replaced with time to market, and we hear sayings and posturing replace the more considered discourse that might lead to better information to more people. Sayings and tag lines is not a new phenomenon. “Win with Wilke”, “I Like Ike”, and “Honest Abe” have always been with us. But the ability to manipulate more people more quickly than ever before is a result of the Internet and the 24-hour news media.

The weapons of influence and the effect of their use on a national scale can be seen in the coverage of the Iowa Straw Poll. First place went by a narrow margin to Michelle Bauchman, with 2nd

place going to Ron Paul, and everyone else a distant 3rd. But the news cycle that followed put the top contenders in the race as Rick Perry, who wasn't even in the straw poll, Mitt Romney, who was an also ran, and Michelle Bauchman, leaving out Ron Paul entirely. The media decided in advance that he was a marginal candidate and essentially pushed him out of the race, favoring someone who didn't participate and someone who finished a long distance behind. This cannot be seen as fair, honest, or accurate reporting, and yet the only media outlet that pointed it out was the Comedy Channel through the Daily Show with John Stewart. Only after Stewart pointed this out by lambasting the so-called legitimate media, did they start to mention Ron Paul, and by then it was too late to undo the influence they had already pushed into the public.

No government controls exist, and there is a strong desire no to control the media from the government because of the propaganda effects. But clearly, the government is not required in order to have propaganda. The major media outlets that control the vast majority of the public perspectives are controlled by major corporations that impose their views through editorial control at a tactical level through their editors and at a strategic level by who they hire and retain. The laws that kept single owners from dominating the media in the US have been largely swept away over time, and thus the public discourse is inherently limited and controlled by the ultra rich.

The battle for the Internet

An ongoing battle in the influence war is currently underway for control of the Internet as a media. It is a similar battle to the one that was fought and won by the monied interests in the broadcast media. At the center of this battle you find Lauren Weinstein[41] and others who seek to counter the monied interests through purely informational tactics. But it seems unlikely that those with few resources will often or long win such a battle, and those with the finances to prosecute this element of the war can continue the battle for as long as it takes, and in a wide range of different approaches. The ultimate question seems to be what the powerful and well resources elements of society want from the Internet and how they will go about getting it.

41 http://www.pfir.org

While it seems unlikely that efforts in the short run will silence those who seek freedom for information and equality for those who wish to access and provide it, silence is not necessary in order to win the influence battle. If the fear of cyber terrorism, cyber crime, cyber warfare, or whatever comes next won't get it done, something else will. While freedoms long held are slow and hard to remove, freedoms that never were are easily dismissed. China never had a free Internet, and it is advancing at a rapid pace. Even if some protesters remains and even if technical means to bypass controls are still in place, this has little effect on the masses that determine elections, support governments, and control means of production. If you want a good job, you will still have to bow down to a corporate interest or work in an area that they don't care to influence. The whistle blowers almost all end up out of the mainstream and unable to influence the long-term future, while those they make their claims against almost always continue to prosper long after the consequences of the few bad acts they were caught at. There are exceptions that disprove the rule, but the odds favor the wealthy and powerful and the information age has not changed this.

The battle for the Internet is raging still, and anticipating the result is a poor bet to make. The key to the future though is not in the low-level protests, but the capacity to influence the key decision-makers. Like it or not, policy at a global and national level is set by and sets the future of influence tactics. Which of the rich and powerful concerns battling it out for control will win and what will their political philosophy bring with it? Will they even bother to think it through? The media is both the weapon and the ultimate target of the weapon. The Internet will be used to influence the decision-makers, who in turn will influence the future of the Internet. But the broadcast media will make it harder for Internet freedom fighters.

The hearts and minds

At every level, the battle rages, and the weapons today are still in their infancy. If the Internet battle is lost before the weapons of influence are well built out, the outcomes will be far different than if the weapons are built first and the battle then fought. There is an arms race underway, and it exists at every level of the influence stack - from the individuals fighting it out for small niches of survival to the strategic battles between nation-states and global

corporations for control over the mindset of humanity for the coming centuries. Which ideologies will win is not set only by the strength of the ideologies, but the strength of the weapons used to wage the battles and the war. Will capitalism in its pure form win out over the balance of antitrust and lead to the new oligarchs? Which religions will dominate decision-making in which areas of the World? Will a global government arise and what form will it take? These are questions not likely to be answered by fundamental differences between the alternatives, but rather by the weapons of influence they apply and the strength of the understanding and vision of those who wield these weapons.

The battle for the truth and the issues of time

Perhaps the most important question to address in the influence war is whether and to what extent truth will prosper. War has a way of concealing the truth, mangling it into unrecognizable reflections suited to the desired of leaders and their support groups, being protected by a "bodyguard of lies", and so forth. One widespread belief is that the VietNam "war"[42] was "lost"[43] by the US because those favoring peace showed the bodies of dead soldiers being brought home every day. In the "war" in Iraq, this "mistake" was not repeated, and one view is that this resulted in more and longer support for that war, enabling it to be "won".[44] The issues are, of course, far more complex than this simplistic explanation.

The influence arena is, in essence, a giant and complicated control system. It has many actors seeking to influence others at all levels, and the event sequences that take place in the information arena dictate which sets of people buy into which sets of ideas over time. We know from scientific research that the influence patterns are strongest when they reflect combinations of emotions and that new concepts and ideas are most reflected in the long run by the first impressions the listeners have of them. In essence, this aspect of influence warfare comes down to a race. Whoever makes the best emotional appeal and most compelling meme the fastest is the

42 This war – as all wars today – was not declared so by law.
43 The question as to weather a peace accord is a "loss" seems relevant.
44 This undeclared war was also settled by a peace accord, but with the new government – hence the win.

short-term winner, and if the memes can hold up until the fait-a-complit time ends, has by far the best chance of winning the issue.

In elections, it is increasingly better to be newer to the political scene than older, because there is less past to dig up and digging it up takes longer. Limiting media exposure makes it harder to show weaknesses, while coming out with great sayings and being able to back them up to one level of detail it all that's needed to make compelling case after compelling case. And in many cases, it doesn't even take that much.

The race is between the speed with which people can spread their influences and the speed with which the truth can be discerned from everything else. Winning the race for better information largely means winning the hearts and minds of the population. If those who would spread fear, loathing, discontent, happiness, joy, pleasure, and other emotions associated with desired points of view through deception can be countered by honest evaluations that have sufficient force in sufficient time, then truth will win out over delusion and people will make decisions based on their understandings of that truth. Otherwise, regardless of any real merit a point of view has, the charismatic leaders will battle it out for mindshare with no connection to reality involved.

Arguably, better information may not lead to better decisions. But as a personal matter, and as a general rule, I believe that better decisions come from better information. An honest decision-maker who is willing to consider the available information and has more accurate information presented in a fair manner will more often make a better decision in terms of forwarding their objectives than the same decision-maker given less accurate information or information presented in a more skewed manner. For a dishonest decision-maker or one unwilling to consider the relevant information the outcomes will likely remain skewed.

At some point, decisions must be made and actions taken. And at this point, the only information considered is the information available. If better information comes later, it simply doesn't matter.

Winning the race by better information is then the key strategic issue in winning the influence war. Regardless of what your

objectives are, if you get better information faster, all other things being equal, you are more likely to win.

Winning the race and the associated weaponry

The race for getting better information sooner requires advanced information weapons. In the advertising game, discerning who will buy and when has led to high valued real-time analytics that allow advertisers to make automated decisions in milliseconds about what advertisements to put in front of buyers about to act. In the financial industries, investment decisions that take advantage of momentary differentials in value race against each other with the fastest order winning that much more return on their investment. Google now provides type-ahead and preview results before the user finishes typing each word, presumably anticipating the questions we are about to ask of it based on its analysis of its previous interactions with us.

These microcosms are only the tip of the coming iceberg. As the push for real-time information rages, better information faster is driving the information technology to extremes. The influence weaponry of the future will have to meet these challenges on a global scale, in time frames transparent to the human targets of influence, and with responses appropriate to the policies set by the leaders involved.

This means, at a minimum, and in human real-time timeframes, the ability to:

- Read and understand, at some level of detail, the content of structured and unstructured communications, and its effects on the perceptions of targets of influence of all relevant parties.
- Analyze influences and their effects on all parties to the level of granularity and over the domains of discourse important to the issues of influence.
- Determine a suitable course of action in terms of countering or supporting those influences identified.

- Induce actions that support desired and counter undesired influences with attention to both the tactical and strategic situation.
- To the extent that truth is a desired property, this also involves doing these things so as to project only truthful influences to all of the target audiences.

This control system is not likely to appear soon, but research into the issues is already underway around the world. In the competition between enterprises ranging from major corporations to startup companies, in the religious orders of the world, and in the research and development departments of nation states and sub state-actors, these issues are increasingly coming to the fore.

These emerging weapons of war also integrate with and have effect upon the other weaponry of the day. The use of so-called smart weapons that serve more certain death with less collateral damage are not just about some financial efficiency. They are about influencing the affected population toward the belief that the wielders of those weapons are just and fair. Compare this to the ancient art of war where destruction of the village which failed to expel the enemy was considered a sound path to influencing other villages to decide which side they were on as the invading force came closer to the gates.

The other side of these weapons is perhaps even more problematic to many desiring free, open, and private speech. In order to kill off “terrorists” and their plots, government around the world are placing sensors of all sorts throughout public spaces, as companies are placing similar sensors within their private spaces, and individuals increasingly have and use nanny-cams and other surveillance technologies within their homes. These “security” systems are in fact surveillance systems that offer the hope of catching more and more of the “bad guys” sooner.

Of course when after the fact becomes too late, they become weapons of anticipation rather than response, and start to act as deterrence. Big brother is always watching, and if you speed or go through a red light or spit on the sidewalk, they will catch you on video and come and get you. Having sex in the park now comes with a YouTube video when the park police decide to copy the

surveillance shots and put them on the Web. Technology to peer through walls makes your bedroom subject to external inspection, so the sex police can have you arrested for using an unauthorized position.

Your computer, which you are now legally mandated to use for filing corporate taxes, is being forced to run software from sources authorized by the government to meet their needs. At the same time, the software companies place surveillance technologies in those computers, first to detect stolen copies of music tracks, but ultimately to take and redirect your Internet usage patterns, track and share your notes and letters, and watch your children at home in their bedrooms from the school principle's office. In one form or another, these are all already in place and have already been used. Larry Ellison's assertion that ”privacy is dead” is pretty close to reality when it comes to computer systems. All of this is part and parcel of the influence battle that is ongoing in the Internet environment today. Here are some of the things you are likely to hear:

- If you're innocent, you have nothing to fear.
- There isn't enough time to look at all the surveillance.
- It's only used when a crime has been committed.
- We have to do it to stop the terrorists.

All nice sound bites. All short and sweet and seemingly sensible. And the influence war goes on.

The range from personal interaction to mass media to physiological control over mental state is broad, and there are many sorts of methods and weapons to be applied over that range. Technology today is quite capable of addressing mass media, and over time we will develop the means to detect and respond to different scales of influence campaigns in near real-time, assuming policy decision-makers decide to fund the effort. Public policy and national defense areas will not be funded at the national level by the private sector, but the private sector will continue to fund initiatives to optimize their investments and win in the markets. Which governments in which nation-states decide to fund this area will largely impact which countries prosper in the influence arena. Arguably, the

combination of influence and policy decisions will lead some nation states to prosper and others to fail.

Conclusions

It's not the truth that is at issue in influence, its the ability to sway opinions. And the key question that the influencer has to ultimately answer is where they want the mindset of whom to be set. Once this is understood, the methods of influence may be applied in the marketplace of ideas to seek to move the mindset to the desired set-point, with controls applied through feedback to adapt the influence strategy and tactics with time.

Rudimentary weapons exist today, but as the information age moves forward, the weaponry will grow far more sophisticated and be more individually targetable as to who is affected and in what ways. The challenge of time will ultimately turn the battles pace to one where speed and skill are both necessary in order to prevail. The need for real-time (in human terms) influence responses to influence tactics within a strategic framework will drive up the need for better and better computer-based methods at enormous scales and with an escalating level of effort involved.

In such a situation, the key industrial strength underlying success in the field will be in the areas of computer engineering, software, psychology and sociology, skilled language usage, and technical aspects of information protection. These in turn are driven, in the large scale and over the long run, by the educational capacity of the country wishing to apply them in the key areas of expertise, the funding for applicable research and development in those same areas, and the public's resolve and preparation for the battles ahead.

The foot soldiers of influence operations are not the people pulling the levers of power and influence. They are the people forming the body politic of the country; the groups leaders and followers who move from thought to thought, the members of the media who help drive them in packs toward and away from different viewpoints, and the people themselves and their decisions about when to invest, when to pull back, when to be brave, and when to shrink in fear. And behind them are the skilled specialists who implement the strategies and influence the masses.