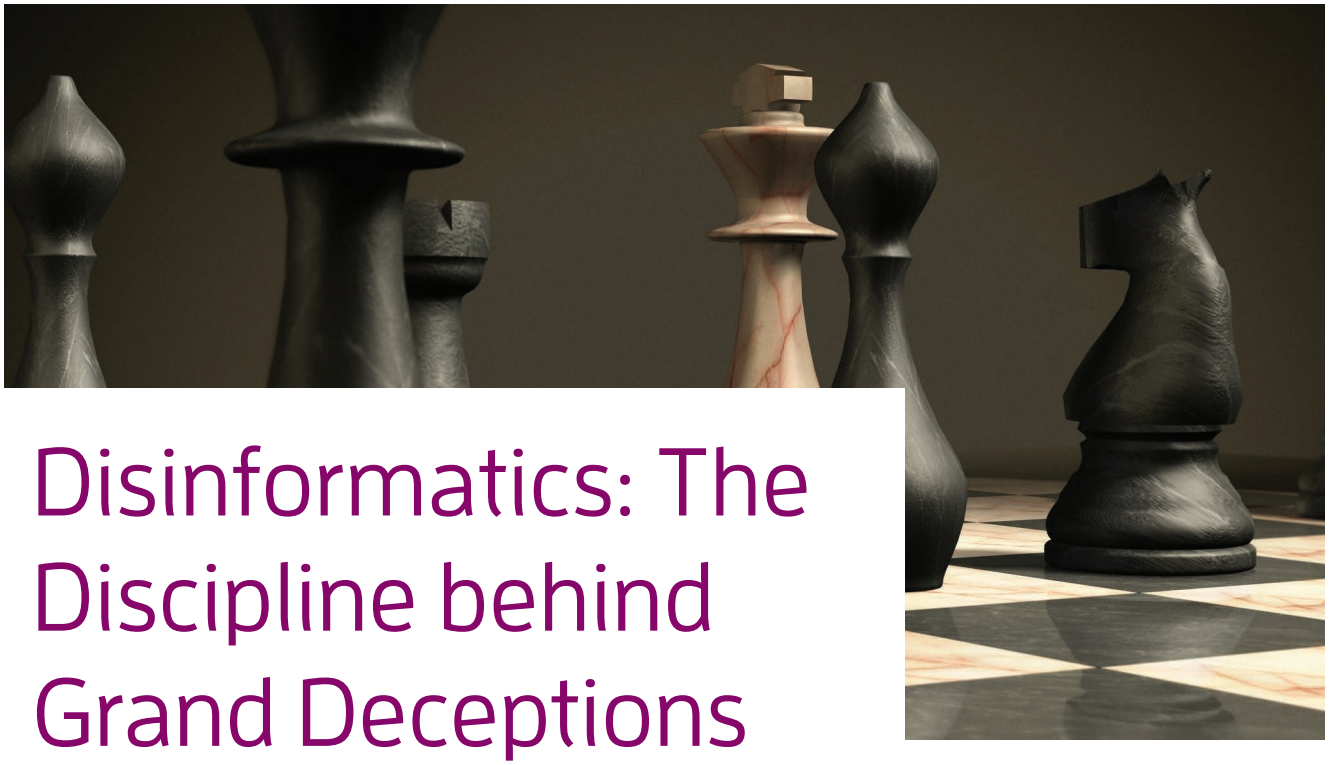
EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org



Disinformatics: The Discipline behind Grand Deceptions

Hal Berghel, University of Las Vegas, Nevada

We need to bring serious study of misinformation and deception into the academy for analysis. A new discipline might be just the vehicle.

Nearly 15 years ago, I had the pleasure of helping to create an interdisciplinary program in informatics, which we defined as the nexus of technology (computers), domain knowledge (biology, science, complex systems, and so on) and people (human–computer interaction, media, social organization, security, and privacy). Today, in light of recent political developments, I'm convinced that we also need to study the darker size of human interaction. I call this prospective new discipline *disinformatics*.

UNKNOWLEDGE AND TRUE BELIEVERS

Simply put, disinformatics is the study of misinformation, broadly defined, and its use (or, if you prefer, information, broadly defined, and its misuse). Disinformatics reveals itself at the intersection of technology, propaganda, and miscreants. It's the glue that holds together modern faux news outlets, AM talk radio, Twitterstorms, and sundry other sorts of sociopolitical babble. It's ideologically grounded in postmodern logic and epistemology (for example, truth is what makes the public strong in body and spirit) and rests upon a foundation of informal logical fallacies and falsehoods.

Should disinformatics qualify as a discipline? The way it's used by ideologues and the controlling elite, it appears so. Peter Denning wrote that disciplines are defined by four hallmarks: a durable domain of human concerns; a codified body of principles (domain knowledge); a codified body of practices; and standards for competence, ethics, and practice.[1] That's a good working definition. Let's examine these conditions one by one.

Disinformatics readily conforms to a durable domain of human concerns. Brief exposure to blustery AM talk-radio hosts will confirm that. The continuous outpouring of fanaticism betrays religious-like zealotry—

a conviction that humanity is headed in the wrong direction and that only a select few of their peers can provide the remedy. And make no mistake about this—they're very serious about their work.

As far as principles go, disinformatics has a common core of strident opinions—what Lewis Carroll might have called *unknowledge*. We'll be quite inclusive in the use of this term. Unknowledge includes fake news, alt-facts, post-truths, partisan politics, anti-science, garden-variety distortions, leaps of faith, and various linguistic and rhetorical devices that support the galvanization and cohesion of opinion:

- Media intimidation and restrictions
- Identification of crises or political paralysis to justify emergency measures
- Attacks on minorities; scapegoating foreigners
- Closing of space for civil society (through funding restrictions, legal cases, raids and arrests, and so on)
- Rhetorical rejection of the current political system; discourse shift
- Expanding the size of courts or other bodies to stack it with partisan judges/officials

> Disinformatics reveals itself at the intersection of technology, propaganda, and miscreants.

lies, intentional deceptions, convenient slips of the tongue, malapropisms, antihistorical narratives, and, of course, the age-old staple of despots and tyrants, BS.[2] Disinformatics epistemology specifically deals with truth in the postmodern sense à la Martin Heidegger: statements that serve the interests of the power elite. Years of human social interaction will show that disinformatics epistemology has been the rule rather than the exception for a good part of human history. Human tribes always relied on unknowledge to resolve major disputes whenever reason failed.

As far as the first two conditions are concerned, our neophyte discipline is looking good. But we need to satisfy two additional conditions: a codified body of practices, and standards for competence, ethics, and practice.

We can extrapolate the former from modern politics, which is well populated with disinformaticians. Political scientist Jeff Colgan makes easy work of extrapolation with his list of warning signs for democratic erosion:[3]

- Modifying rules to impose or eliminate term limits on officials, especially election officials
- Weakening of legislatures/intimidation of legislators
- Silencing of political opposition
- Significant increase in internal security forces

We could modify this list to include distributing information online that isn't fact-checked or vetted by journalists, trolling on social media, and so forth. But the point to bear in mind is that disinformatics is used in service of goals like those enumerated by Colgan and relies primarily on a wide variety of unfiltered distribution mechanisms (such as social media sites). For example, when a politician attempts to de-legitimize a judicial opponent by calling him a "so-called judge" in a tweet, he's using a disinformatics tactic on a social networking platform to silence political opposition. A carefully articulated correspondence between Colgan's work on democratic erosion and our current political experience can be found in a recent book by E.J. Dionne Jr., Norman J. Ornstein, and Thomas E. Mann.[4]

So, with just slight hand waving, we can show that disinformaticians share a loosely knit, core set of practices. But what of standards for competence, ethics, and practice? Once again we have only to look at the behavior of politicians.

Competence is easy. Disinformaticians gauge their competence by winning elections, crushing political opponents, defaming and delegitimizing adversaries, distracting the public from real issues, getting people fired, ruining businesses that oppose their interests—the list is endless. Practice is fairly straightforward as well, for it follows from the observations of George Orwell and Aldous Huxley in the past century. Dionne, Ornstein, and Mann cite Soviet-born journalist Peter Pomerantzev's modern amplification of Orwell/Huxley: "the Kremlin has finally mastered the art of fusing reality TV and authoritarianism to keep the great, 140-million-strong population entertained, distracted, constantly exposed to geopolitical nightmares, which if repeated enough times become infectious." This quote illustrates that the core set of practices are time-honored, widespread, and portable across national boundaries. Huxley and Orwell would be pleased with Pomerantzev.

Ethics, however, presents me with a problem because I've never been able to wrap my mind around the world view of the disinformatician. Frankly, I never really understood why public relations pioneer Edward Bernays became so enamored of propaganda[5] or public opinioneer Frank Luntz found wordsmithing for political manipulation interesting.[6] Bernay's campaign to get women to smoke cigarettes by referring to them as torches of freedom, and Luntz's arousal of the public ire against estate taxes by calling them death taxes, impressed me as both subcerebral and paradigmatically unethical—though presumably

they saw their behavior as acceptable within their own moral framework. Hence, for me, disinformational ethics is like the hunting of endangered species: I don't relate to it, but recognize that it goes on.

So there we have it. Disinformatics has its own body of unknowledge, is propagated by a group of passionate true believers, and has well-defined standards and practices that distinguish the true believers from ideological pagans. There are parallels to earlier, wonky quasi-intellectual pursuits like alchemy, occultism, the miasmatic disease theory, the four humors theory of physiology, astrology, aura reading, the belief in dragons and ghosts, and Area 51 aliens, to name but a few. Just as a blueprint conforms to current architectural standards and building codes, so a disinformatician might claim that certain beliefs conform to current partisan agendas. The vetting process is the same, but the intellectualism is less deep. We don't have to agree with the standards to acknowledge their existence.

Some might object that I'm attaching more prestige to disinformatics than is justified. Perhaps. But I submit that disinformatics is as much a discipline as religion, though one that's agenda rather than faith based. All disciplines function to dissever members from nonmembers for specific reasons—good, bad, or indifferent.

COLLECTIVE LYING AND ENTROPY

Some social scientists have suggested that one of the critical intellectual skills Neanderthals never got right was collective learning: the ability to learn as a group and pass on the information to subsequent generations (www.bighistoryproject.com/chapters/4#intro). That was the key to Hominidae's successful adaptation to the environment. As a result, Neanderthals didn't participate in the Great Leap Forward, and consequently were left behind in the Paleolithic dustbin of history.

There's certainly a ring of truth to this, as dumb bipeds generally lack the ability to compete with other mammals. Our brains are our greatest survival tool. The inability to share knowledge and pass it along destined Neanderthals to compete inefficiently and ineffectively. Collective learning was a milestone for our species: we learned our way out of the Stone Age. Neanderthals, not so much.

Collective lying is the antithesis of collective learning. In the latter case, misinformation displaces knowledge. This is another way of describing fake news: a set of memes that can supplant both knowledge and the search for it. Collective lying introduces more entropy into communication—what we might call the First Law of Disinformatics. But unlike traditional thermodynamics, additional entropy doesn't inevitably lead to information equilibrium. Instead, collective lying produces clumps in info-space. The grand challenge for disinformatics is to account for this phenomenon.

Information theory provides an interesting perspective on collective lying and fake news. Misinformation artificially inflates the entropy of archived data because it introduces new information that appears more or less random. Informally, this is a variation of Claude Shannon's concept of information entropy.[7]

Suppose that all of recorded history is in a single digital library. The percentage of factual information (what corresponds to reality) should increase slightly over time: we don't always get all the facts right the first time, but scholars tend to make corrections to the record—the facts will converge up to a point. Thus, if we honestly and objectively enter data into our library, it should approach equilibrium over time as the mistakes are corrected. We might think of the bits of library information as the atoms that make up each microstate (fact), while the macrostate of the library is its "collective knowledge."

Fake news by definition doesn't cohere with collective knowledge—it is, after all, fake. So when the birthers, Pizzagaters, and Bowling Green massacre merchants pollute the web, blogosphere, or Wayback Machine servers with lies, distortions, and sundry other misinformation, they're necessarily introducing data clumps into the digital broth—clumps that can never mix well with other information because they are inconsistent with it. Our watchphrase is: once a misinformation clump, always a misinformation clump. Digitally, clumps are background noise. We note that misinformation can never be reconciled with the veridical data because it's at once both inconsistent and anomalous. If we take information entropy as the measure of the uncertainty or confusion produced by our library once the misinformation clumps have been added, there's no way to purge or filter them because they haven't been identified as such when they were added. In this way, in our library's arrow of time, entropy never decreases. We can postulate this as the Second Law of Disinformatics.

> The Second Law of Disinformatics: once a misinformation clump, always a misinformation clump.

THE BANALITY OF TRIBALISM

The banality of tribalism derives from Hannah Arendt's concept of the banality of evil. Her thesis was that it's often a mistake to credit repugnant crimes to fanaticism or ideology. They're far

<ALT>-FAQS>

There never seems to be a shortage of examples in IT where incompetence reigns supreme. The recent Equifax hack produced one of the largest and most significant data breaches of personally identifiable information (PII) in history. PII on nearly half of the US adult population was leaked in a data breach, exposing approximately 145 million people to the risk of identity theft and credit fraud. The cause of the breach was both pedestrian and avoidable.[1] In a sense, it would be easier to accept if the breach was due to some zero-day exploit or weapons-grade hack. But, alas, it resulted from poor training, management, and information security policy creation and implementation—the usual suspects when it comes to large data breaches.

As fate would have it, the Equifax CIO and CISO at the time of the hack had credentials to match the quality of Equifax's information security policy and implementation. The CIO had degrees in Russian and business administration, and the CISO had degrees in music composition. Needless to say, they're both being beat up a bit by the media for apparent lack of technical expertise.[2,3] We'll avoid the temptation to heap more cheap shots on these executives for perceived experiential parsimony. Instead, we'll lay the blame where it belongs: the Equifax leadership team and board of directors. The CIO and CISO didn't hire themselves!

This is an all-too-familiar scenario. Executives hire managers who provide inadequate security oversight and a breach results. Subsequently, the managers' credentials are called into question and the search begins for the proverbial scapegoats and sacrificial lambs. This happened in 2012 with the South Carolina Department of Revenue breach,[4] in which hackers used a phishing attack to access approximately 4.5 million taxpayer records from consumers and businesses.[5] In this case, the CIO and the director of the Department of Revenue had to split the blame, because the CISO position was vacant during the previous year. In the case of Chelsea Manning, the target of wrath was an Army private who released thousands of confidential and classified documents and diplomatic cables to WikiLeaks.[6] As this goes to press, the security breach de jour involves Uber's data leak of 57 million unencrypted customer records.[7] The company's chief security officer, who apparently oversaw IT security as well as handled the $100,000 payoff to the hackers, was a former prosecutor without credentials in IT security.[8] Color us surprised at this turn of events!

The list of these breaches seems endless. In each case, the real problem remains unaddressed: it's the responsibility of leadership, whether the midlevel executives of Equifax or those of command rank in CENTCOM, to hire effectively and ensure that information security policies are reasonable, conform to best practices, and are thoroughly vetted and enforced, and that the security budget is adequate to the task. It's all too convenient to blame questionable hires for the consequences of sloppy policies that brought them to the organization in the first place. When these breaches arise, our first question should be: who hired these people?[9] Far too many of these positions are given to C-suite friends. We need to be very clear about our meaning to avoid misunderstanding: while appropriate education and training are neither necessary nor sufficient conditions for success, they do affect the probability. As there's in principle no reason to presume that a computer scientist couldn't compose great chamber music, or a cleric couldn't run a Fortune 500 company, or an attorney couldn't design state-of-the-art chipsets, there's in principle no reason why someone who reads Tolstoy in Russian couldn't be a good CIO or a skilled music composer couldn't be a good CISO, and so on. But from my experience, when it comes to managing technology, out-of-band hires do lower the odds considerably.

References

1. H. Berghel, "Equifax and the Latest Round of Identity Theft Roulette," *Computer*, vol. 50, no. 12, 2017, pp. 72–76.
2. B. Popken, "Equifax Execs Resign; Security Head, Mauldin, Was Music Major," NBC News, 15 Sept. 2017; www.nbcnews.com/business/consumer/equifax-executives-step-down-scrutiny-intensifies-credit-bureaus-n801706.
3. B. Fung, "Equifax Security Chief Had Some Big Problems. Being a Music Major Wasn't One of Them.," *The Washington Post*, 19 Sept. 2017; www.washingtonpost.com/news/the-switch/wp/2017/09/19/equifaxs-top-security-exec-made-some-big-mistakes-studying-music-wasnt-one-of-them.
4. H. Berghel, "The SCDOR Hack: Great Security Theater in Five Stages," *Computer*, vol. 46, no. 3, 2013, pp. 91–93.
5. M. Long, "A Year Later, an 'Active' Investigation—but Few Leads—in SCDOR Hacking," South Carolina Radio Network, 21 Oct. 2013; www.southcarolinaradionetwork.com/2013/10/21/one-year-later-active-investigation-but-still-few-leads-in-scdor-hacking.
6. H. Berghel, "WikiLeaks and the Matter of Private Manning," *Computer*, vol. 45, no. 3, 2012, pp. 86–89.
7. J.C. Wong, "Uber Concealed Massive Hack That Exposed Data of 57M Users and Drivers," *The Guardian*, 22 Nov. 2017; www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.
8. E. Newcomer, "Uber Paid Hackers to Delete Stolen Data on 57 Million People," Bloomberg Technology, 21 Nov. 2017; www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.
9. H. Berghel, "The Cost of Having Analog Executives in a Digital World," *Comm. ACM*, vol. 42, no. 11, 1999, pp. 11–13.

more likely committed by unthinking people without benefit of a reliable moral compass who are simply following orders—go-along-to-get-along types. Arendt was specifically referring to Adolf Eichmann's war crimes at his trial in Israel in 1963,[8] but her observation is applicable well beyond the Nazi holocaust. In fact, it seems to apply to tribalism and herd mentalities generally. Eichmann was a joiner—he wanted to be part of the tribe with which he most closely identified. Presumably, such attachment elevates one's sense of self-worth—you're not just one person anymore, but a part of a movement. Add to this a hefty dose of right-wing authoritarianism and a strong social dominance orientation, and mix in some Führerprinzip, and you can account for a good part of political history.[9]

DISINFORMATION AND POLITICS

Disinformation stands to modern political campaigns as dark energy stands to modern cosmology. It permeates politics and accounts for unpredictable outcomes, but we really don't understand it yet—hence the need for the study of disinformatics. Like its baryonic cousin, disinformation is very difficult to identify and measure accurately because of its minimal density compared to reliable data input from other sources like academic journals, reliable news media, and so on. Based on the recent US presidential election, despite the minimal density with respect to the totality of campaign coverage, it seemed to have a dominating influence. Disinformation has become a pervasive, unquantifiable force that dominates much of politics. It manifests itself in manifold ways, and appears in many guises, including troll energy, Twitter litter, alt-facts, and fake news. Without disinformation, it's impossible to account for the anomalies of modern politics, specifically including the elections of the current crop of uninformed, misguided, illogical, and deceitful politicians. As with dark energy, we don't as yet have a means of demonstrating causality, but without it we lose explanatory and predictive capacity. The failure of presidential polling shows that.

Pulitzer Prize–winning journalist Walter Lippmann once remarked: "When distant and unfamiliar and complex things are communicated to great masses of people, the truth suffers a considerable and often a radical distortion. The complex is made over into the simple, the hypothetical into the dogmatic, and the relative into an absolute" (www.brainyquote.com/quotes/walter_lippmann_151318). Disinformatics is the discipline that facilitates this phenomenon.

REFERENCES

1. P.J. Denning, "The Profession of IT: Who Are We?," *Comm. ACM*, vol. 44, no. 2, 2001, pp. 15–19.
2. H. Berghel, "Alt-News and Post-Truths in the 'Fake News' Era," *Computer*, vol. 50, no. 4, 2017, pp. 110–114.
3. J. Colgan, "Risk of Democratic Erosion—Reading List," Nov. 2016; docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxqZWZmZGNvbGdhbnxneDozN2RmZGMzMmEyOWRmNjM5.
4. E.J. Dionne Jr., N.J. Ornstein, and T.E. Mann, *One Nation after Trump: A Guide for the Perplexed, the Disillusioned, the Desperate, and the Not-Yet Deported*, St. Martin's Press, 2017.
5. E. Bernays, *Propaganda*, lg Publishing, 2004.
6. F. Luntz, *Words That Work: It's Not What You Say, It's What People Hear*, reprint ed., Hachette Books, 2008.
7. C.E. Shannon and W. Weaver, *The Mathematical Theory of Communication*, Univ. of Illinois Press, 1971.
8. H. Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil*, Viking, 1963.
9. J.W. Dean, *Conservatives without Conscience*, Viking, 2006.

HAL BERGHEL is an IEEE and ACM Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.