XP GROUP AND RELATED PLAINTIFFS GROUP

Evidence Set, per BRANCHES public
law center http://www.globalscoop.net Case # 2788-D

In pro per Claimant and Plaintiff group requesting Court Appointed legal counsel or the provision of contingency litigators or deferral fee litigators

UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re	:	Chapter 11
Gawker Media LLC, *et al.*, [1]	:	Case No. 16-11700 (SMB)
Debtors.	:	(Jointly Administered)

AMENDED RICO (Racketeer Influenced and Corrupt Organizations Act) DEMAND FOR CO-OPERATIVE FILING OF RICO CHARGES WITH ASSISTED AND ASSOCIATED CHARGES COMBINING THE U.S. DEPARTMENT OF JUSTICE AND PLAINTIFFS AS PLAINTIFF GROUP

WHEREAS, Defendants Gawker Media, GMGI, Gawker Hungary (f/k/a Blogwire Hungary Szellemi Alkotast Hasznosito Kft.), Gawker Entertainment LLC, Gawker Technology, LLC, Gawker Sales, LLC, Nicholas G. A. Denton, Irin Carmon, Univision Communications, Univision America, Adrian Covert, Jon Herrman, Gaby Darbyshire, UniModa LLC, Elon Musk, John Doerr and DOES I through 220, including each employee of Gawker Media, did engage in RICO statute violations in their attempts to damage Plaintiffs.

WHEREAS, public officials and investigators have provided proof of RICO violations to all journalism, Congressional and law enforcement parties with jurisdiction in these charges.

WHEREAS, public news media and IT forums have now confirmed that due to Gawker Media's attempted media manipulations in the 2008 and 2016 Presidential elections and the cross-national exchange of funds and interests between multiple questionable entities on multiple continents that each and every member of the above-stated defendants group has been under electronic surveillance on

1 The last four digits of the taxpayer identification number of the debtors are: Gawker Media LLC (0492); Gawker Media Group, Inc. (3231); and Gawker Hungary Kft. (f/k/a Kinja Kft.) (5056). Gawker Media LLC and Gawker Media Group, Inc.'s mailing addresses are c/o Opportune LLP, Attn: William D. Holden, Chief Restructuring Officer, 10 East 53rd Street, 33rd Floor, New York, NY 10022. Gawker Hungary Kft.'s mailing address is c/o Opportune LLP, Attn: William D. Holden, 10 East 53rd Street, 33rd Floor, New York, NY 10022.

every electronic device with an IMEI address or network functionality by multiple law enforcement, defense, civil investigation, intelligence entities and the placement of under-cover journalists with Defendants group; and that the results of that surveillance, since 2007 is subpoena-accessible in this matter. Further, each of those legitimate entities that engaged in such surveillance that had even a single Cisco or Juniper Networks back-door embedded device touching their network has been revealed by U.S. DHS public reports to have had their servers breached by hackers. Any such evidence discovered after-the-fact may also legally be used in this case as evidence

WHEREAS the publication known as THE INTERCEPT is funded by Gawker Media's backers and shares real-estate venues with Gawker Media, First Look, The Intercept and other coordinating publications and that publication has published the following overview which describes in detail the Stasi-like methods used by Defendants against Plaintiffs:

"One of the many pressing stories that remains to be told from the Snowden archive is how western intelligence agencies are attempting to manipulate and control online discourse with extreme tactics of deception and reputation-destruction. It's time to tell a chunk of that story, complete with the relevant documents.

Over the last several weeks, I worked with *NBC News* to publish a series of articles about "dirty trick" tactics used by GCHQ's previously secret unit, JTRIG (Joint Threat Research Intelligence Group). These were based on four classified GCHQ documents presented to the NSA and the other three partners in the English-speaking "Five Eyes" alliance. Today, we at *the Intercept* are publishing another new JTRIG document, in full, entitled "The Art of Deception: Training for Online Covert Operations."

By publishing these stories one by one, our NBC reporting highlighted some of the key, discrete revelations: the monitoring of YouTube and Blogger, the targeting of Anonymous with the very same DDoS attacks they accuse "hacktivists" of using, the use of "honey traps" (luring people into compromising situations using sex) and destructive viruses. But, here, I want to focus and elaborate on the overarching point revealed by all of these documents: namely, that these agencies are attempting to control, infiltrate, manipulate, and warp online discourse, and in doing so, are compromising the integrity of the internet itself.

Among the core self-identified purposes of JTRIG are two tactics: **(1)** to inject all sorts of false material onto the internet in order to destroy the reputation of its targets; and **(2)** to use social sciences and other techniques to manipulate online discourse and activism to generate outcomes it considers desirable. To see how extremist these programs are, just consider the tactics they boast of using to achieve those ends: "false flag operations" (posting material to the internet and falsely attributing it to someone else), fake victim blog posts (pretending to be a victim of the individual whose reputation they want to destroy), and posting "negative information" on various forums. Here is one illustrative list of tactics from the latest GCHQ document we're publishing today:

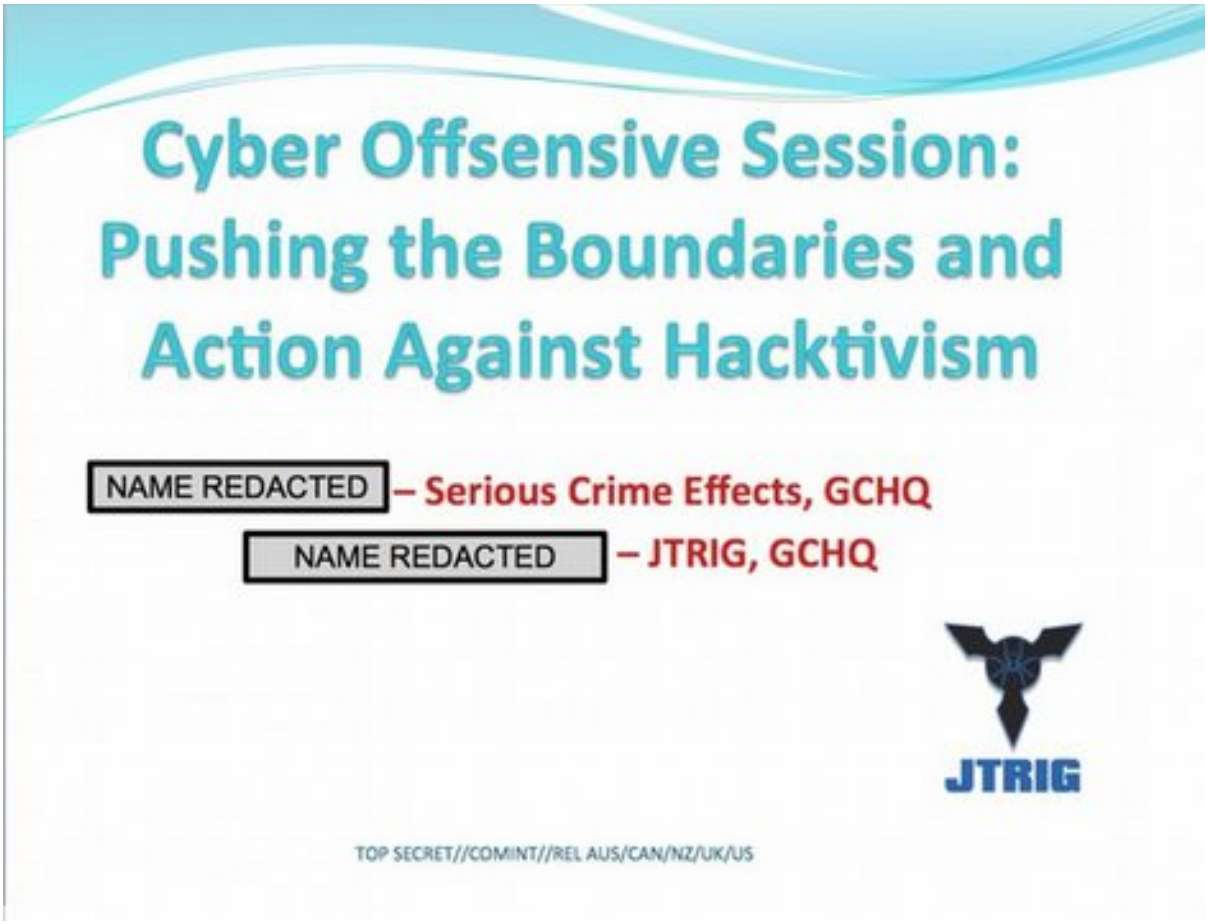
Other tactics aimed at individuals are listed here, under the revealing title “discredit a target”:

Then there are the tactics used to destroy companies the agency targets:

GCHQ describes the purpose of JTRIG in starkly clear terms: “using online techniques to make something happen in the real or cyber world,” including “information ops (influence or disruption).”

Critically, the "targets" for this deceit and reputation-destruction extend far beyond the customary roster of normal spycraft: hostile nations and their leaders, military agencies, and intelligence services. In fact, the discussion of many of these techniques occurs in the context of using them in lieu of "traditional law enforcement" against people suspected (but not charged or convicted) of ordinary crimes or, more broadly still, "hacktivism", meaning those who use online protest activity for political ends.

The title page of one of these documents reflects the agency's own awareness that it is "pushing the boundaries" by using "cyber offensive" techniques against people who have *nothing to do with terrorism or national security threats*, and indeed, centrally involves law enforcement agents who investigate ordinary crimes:



No matter your views on Anonymous, "hacktivists" or garden-variety criminals, it is not difficult to see how dangerous it is to have secret government agencies being able to target any individuals they want – **who have never been charged with, let alone convicted of, any crimes** – with these sorts of online, deception-based tactics of reputation destruction and disruption. There is a strong argument to make, as Jay Leiderman demonstrated in *the Guardian* in the context of the Paypal 14 hacktivist persecution, that the "denial of service" tactics used by hacktivists result in (at most) trivial damage (far less than the cyber-warfare tactics favored by the US and UK) and are far more akin to the type of political protest protected by the First Amendment.

The broader point is that, far beyond hacktivists, these surveillance agencies have vested themselves with the power to deliberately ruin people's reputations and disrupt their online political activity even though they've been charged with no crimes, and even though their actions have no conceivable connection to terrorism or even national security threats. As Anonymous expert Gabriella Coleman of McGill University told me, "targeting Anonymous and hacktivists amounts to targeting citizens for expressing their political beliefs, resulting in the stifling of legitimate dissent." Pointing to this study she published, Professor Coleman vehemently contested the assertion that "there is *anything* terrorist/violent in their actions."

Government plans to monitor and influence internet communications, and covertly infiltrate online communities in order to sow dissension and disseminate false information, have long been the source

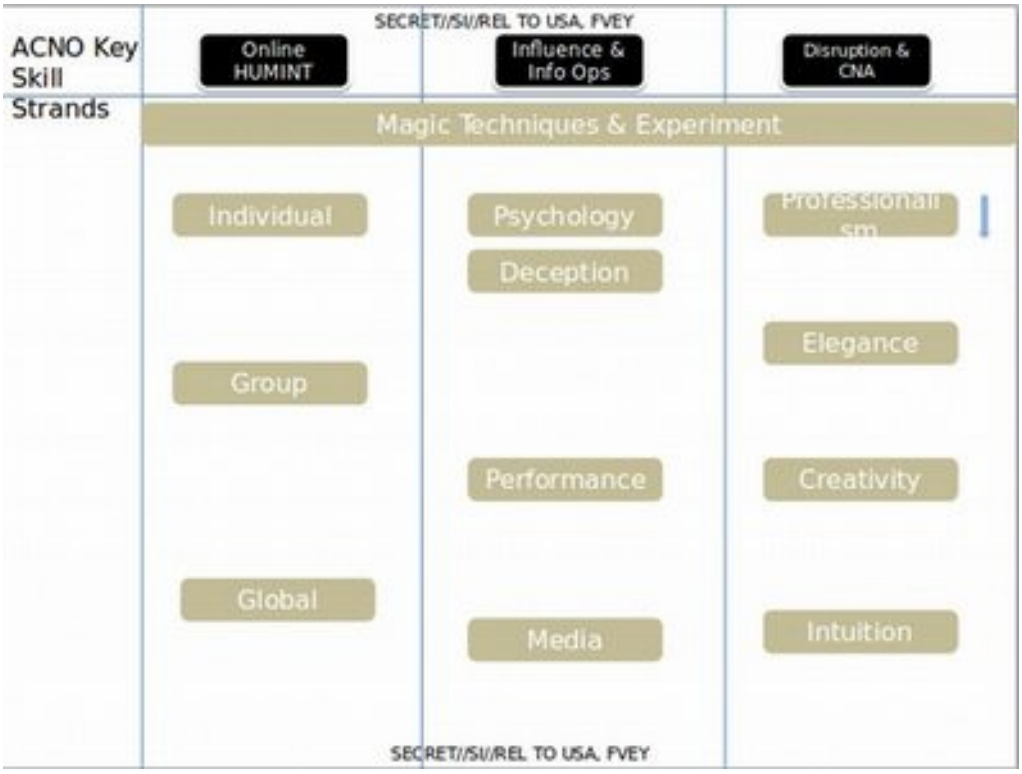
of speculation. Harvard Law Professor Cass Sunstein, a close Obama adviser and the White House's former head of the Office of Information and Regulatory Affairs, wrote a controversial paper in 2008 proposing that the US government employ teams of covert agents and pseudo-"independent" advocates to "cognitively infiltrate" online groups and websites, as well as other activist groups.

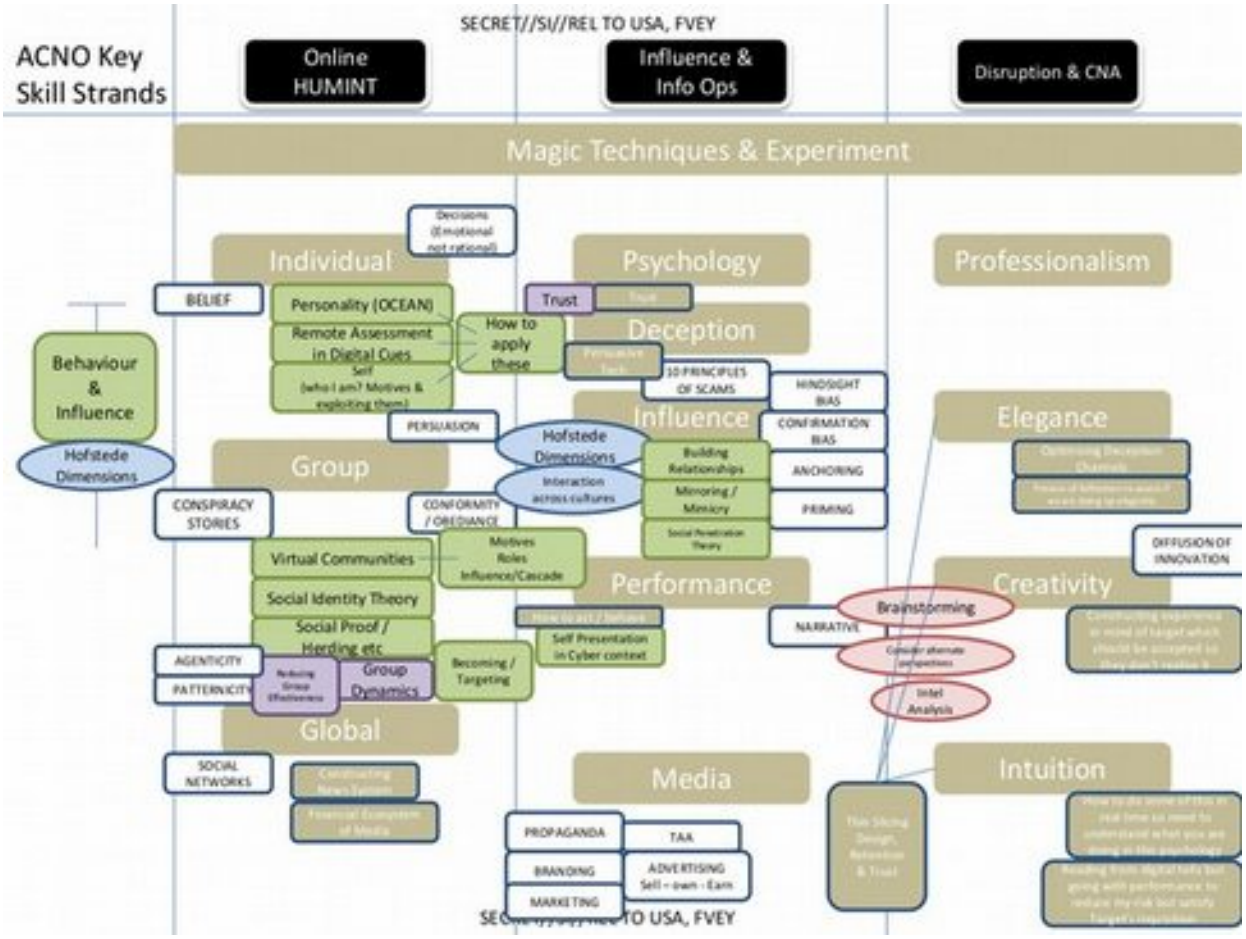
Sunstein also proposed sending covert agents into "chat rooms, online social networks, or even real-space groups" which spread what he views as false and damaging "conspiracy theories" about the government. Ironically, the very same Sunstein was recently named by Obama to serve as a member of the NSA review panel created by the White House, one that – while disputing key NSA claims – proceeded to propose many cosmetic reforms to the agency's powers (most of which were ignored by the President who appointed them).

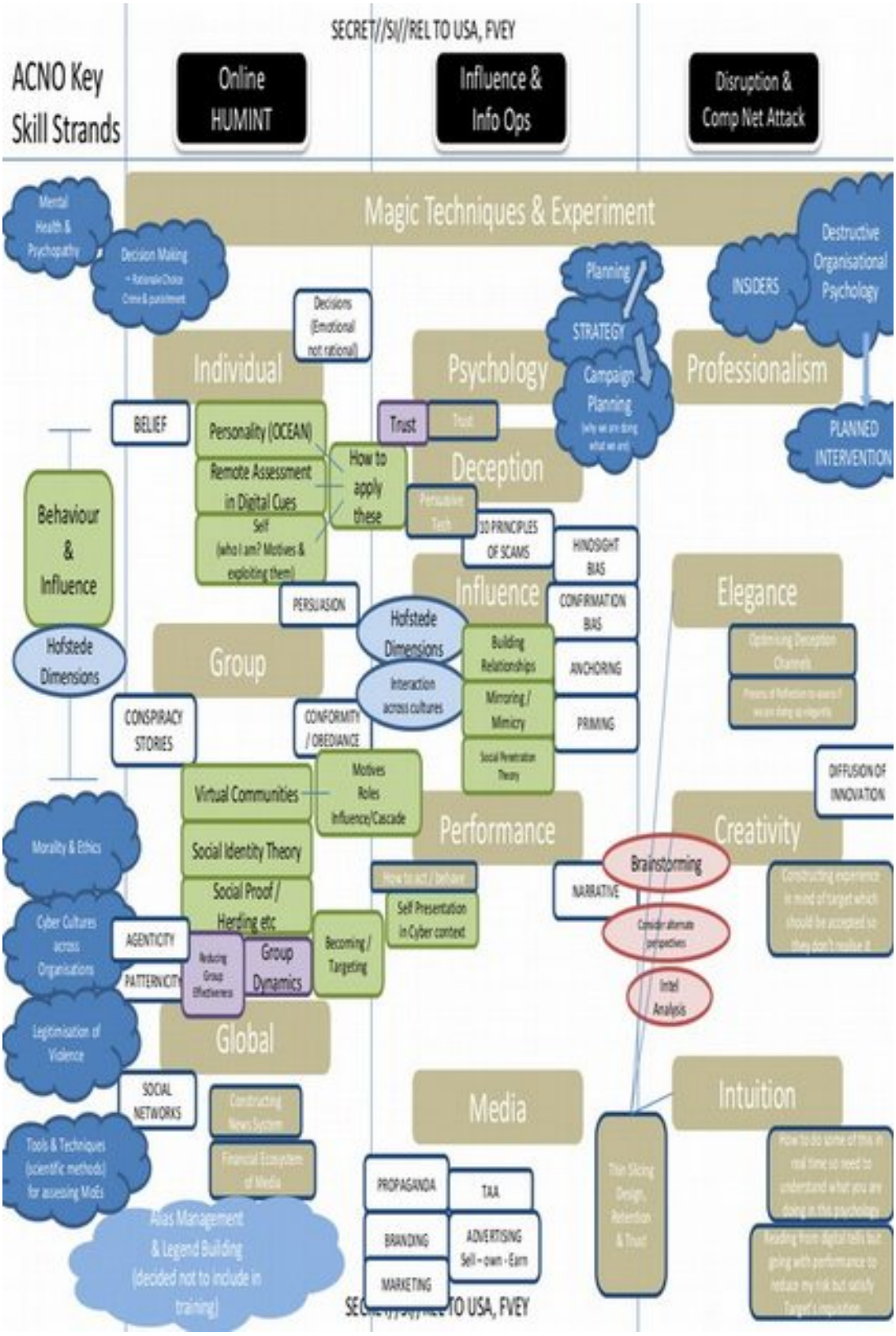
But these GCHQ documents are the first to prove that a major western government is using some of the most controversial techniques to disseminate deception online and harm the reputations of targets. Under the tactics they use, the state is deliberately spreading lies on the internet about whichever individuals it targets, including the use of what GCHQ itself calls "false flag operations" and emails to people's families and friends. Who would possibly trust a government to exercise these powers at all, let alone do so in secret, with virtually no oversight, and outside of any cognizable legal framework?

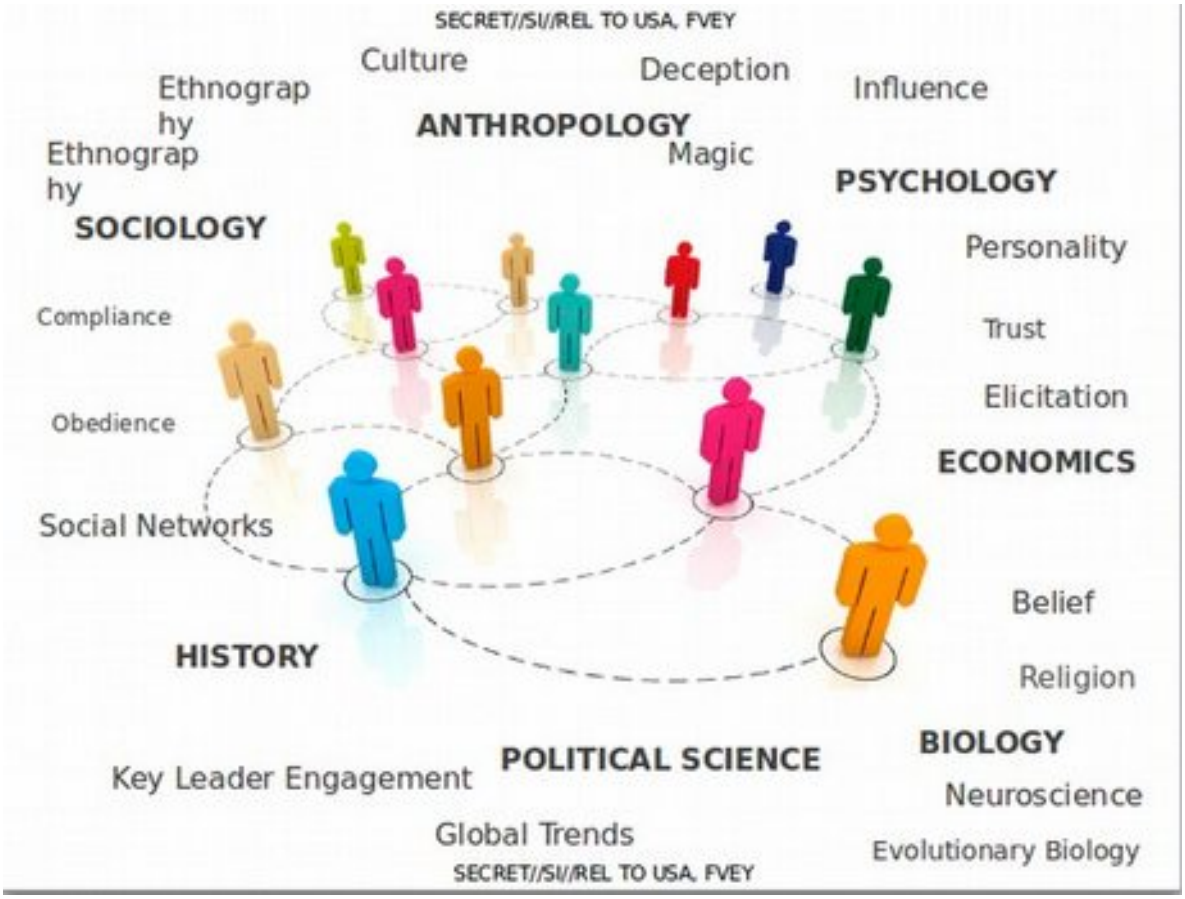
Then there is the use of psychology and other social sciences to not only understand, but shape and control, how online activism and discourse unfolds. Today's newly published document touts the work of GCHQ's "Human Science Operations Cell," devoted to "online human intelligence" and "strategic influence and disruption":

Under the title “Online Covert Action”, the document details a variety of means to engage in “influence and info ops” as well as “disruption and computer net attack,” while dissecting how human beings can be manipulated using “leaders,” “trust,” “obedience” and “compliance”:


SECRET//SI//REL TO USA, FVEY
ACNO Key Skill Strands
Online HUMINT
Influence & Info Ops
Disruption & CNA
Magic Techniques & Experiment
Individual
Psychology
Professionalism
Deception
Elegance
Group
Performance
Creativity
Global
Media
Intuition
SECRET//SI//REL TO USA, FVEY


SECRET//SI//REL TO USA, FVEY
ACNO Key Skill Strands
Online HUMINT
Influence & Info Ops
Disruption & CNA
Magic Techniques & Experiment
Individual
Psychology
Professionalism
Deception
Influence
Elegance
Group
Performance
Creativity
Global
Media
Intuition
Behaviour & Influence
Hofstede Dimensions
BELIEF
Personality (OCEAN)
Remote Assessment in Digital Cues
Self (who I am? Motives & exploiting them)
How to apply these
Trust
PERSUASION
10 PRINCIPLES OF SCAMS
HINDSIGHT BIAS
CONFIRMATION BIAS
ANCHORING
PRIMING
Building Relationships
Mirroring / Mimicry
Hofstede Dimensions
Interaction across cultures
CONSPIRACY STORIES
CONFORMITY / OBEDIANCE
Motives Roles Influence/Cascade
Virtual Communities
Social Identity Theory
Social Proof / Herding etc
AGENTICITY
PATTERNICITY
Group Dynamics
Becoming / Targeting
Self Presentation in Cyber context
NARRATIVE
Brainstorming
Intel Analysis
DIFFUSION OF INNOVATION
SOCIAL NETWORKS
PROPAGANDA
TAA
BRANDING
ADVERTISING
MARKETING
Sell - learn - Earn


SECRET//SI//REL TO USA, FVEY
ACNO Key Skill Strands
Online HUMINT
Influence & Info Ops
Disruption & Comp Net Attack
Magic Techniques & Experiment
Mental Health & Psychopathy
Decision Making
Decisions (Emotional not rational)
Planning
STRATEGY
Campaign Planning
INSIDERS
Destructive Organisational Psychology
PLANNED INTERVENTION
Individual
Psychology
Professionalism
BELIEF
Personality (OCEAN)
Remote Assessment in Digital Cues
Self (who I am? Motives & exploiting them)
How to apply these
Trust
Deception
Persuasive Tech
10 PRINCIPLES OF SCAMS
HINDSIGHT BIAS
Behaviour & Influence
PERSUASION
Influence
CONFIRMATION BIAS
Elegance
Hofstede Dimensions
Hofstede Dimensions
Group
Building Relationships
ANCHORING
Interaction across cultures
Mirroring / Mimicry
PRIMING
CONSPIRACY STORIES
CONFORMITY / OBEDIANCE
Social Penetration Theory
DIFFUSION OF INNOVATION
Virtual Communities
Motives Roles Influence/Cascade
Performance
Creativity
Morality & Ethics
Social Identity Theory
Brainstorming
NARRATIVE
Social Proof / Herding etc
Self Presentation in Cyber context
Cyber Cultures across Organisations
AGENTICITY
PATTERNICITY
Reducing Group Effectiveness
Group Dynamics
Becoming / Targeting
Consider alternate perspectives
Intel Analysis
Legitimisation of Violence
Global
SOCIAL NETWORKS
Media
Intuition
Tools & Techniques (scientific methods) for assessing MoEs
PROPAGANDA
TAA
BRANDING
ADVERTISING Sell - own - Earn
MARKETING
Alias Management & Legend Building (decided not to include in training)
SECRET//SI//REL TO USA, FVEY

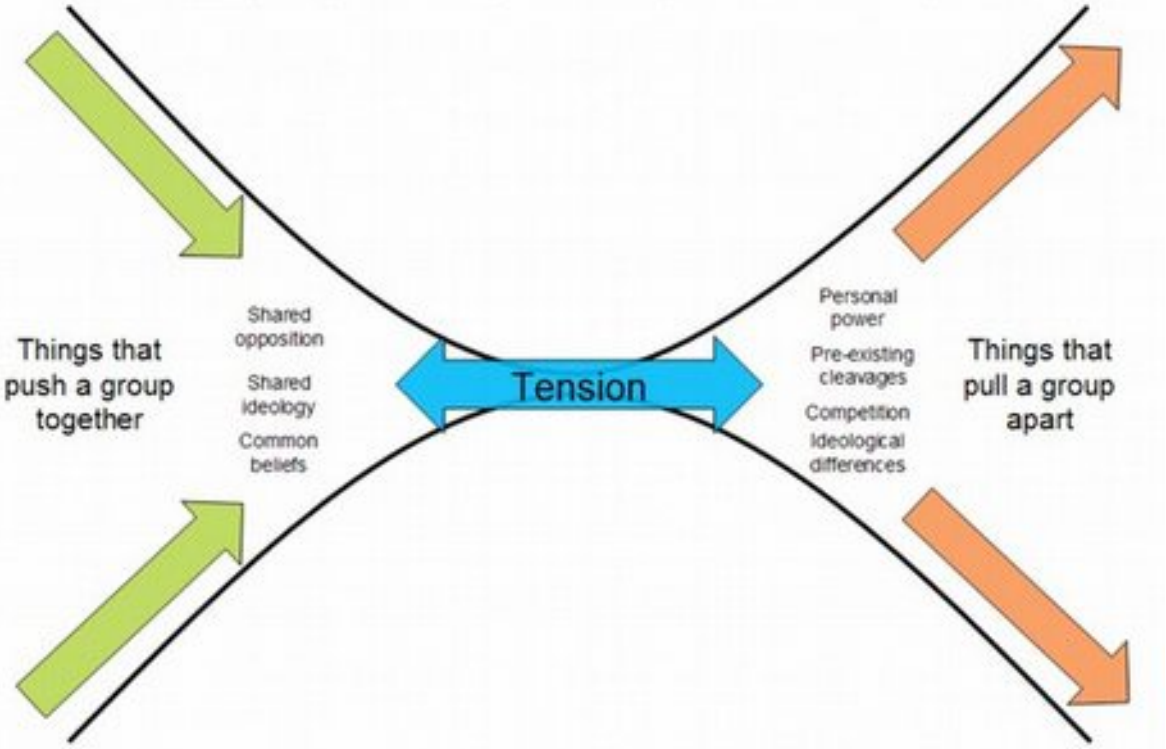


The documents lay out theories of how humans interact with one another, particularly online, and then attempt to identify ways to influence the outcomes – or "game" it:

Gambits for Deception

Attention	Control attention Conspicuity & Expectancies	The big move covers the little move	The Target looks where you look	Attention drops at the perceived end	Repetition reduces vigilance
Perception	Mask/Mimic Eliminate - Blend Recreate - Imitate	Repackage/Invent Modify old cues Create new cues	Dazzle/Decoy Blur old cues Create alternate cues	Make the cue dynamic	Stimulate multiple sensors
Sensemaking	Exploit prior beliefs	Present story fragments	Repetition creates expectancies	Haversack Ruse (The Piece of Bad Luck)	Swap the real for the false, & vice versa
Affect	Create Cognitive Stress	Create Physiological Stress	Create Affective Stress (+/-)	Cialdini+2	Exploit shared affect
Behaviour	Simulate the action	Simulate the outcome	Time-shift perceived behaviour	Divorce behaviour from outcome	Channel behaviour

Identifying & Exploiting fracture points



SECRET//SI//REL TO USA, FVEY

Mirroring

People copy each other while in social interaction with them.

- body language
- language cues
- expressions
- eye movements
- emotions

Accommodation

Adjustment of speech, patterns, and language towards another person in communications

- People in conversation tend to converge
- Depends on empathy and other personality traits
- Possibility of over-accommodation and end up looking condescending

Mimicry

adoption of specific social traits by the communicator from the other participant

Question: Can I game this?

SECRET//SI//REL TO USA, FVEY

We submitted numerous questions to GCHQ, including: (1) Does GCHQ in fact engage in “false flag operations” where material is posted to the Internet and falsely attributed to someone else?; (2) Does GCHQ engage in efforts to influence or manipulate political discourse online?; and (3) Does GCHQ’s mandate include targeting common criminals (such as boiler room operators), or only foreign threats?

As usual, they ignored those questions and opted instead to send their vague and nonresponsive boilerplate: “It is a longstanding policy that we do not comment on intelligence matters. Furthermore, all of GCHQ’s work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight, including from the Secretary of State, the Interception and Intelligence Services Commissioners and the Parliamentary Intelligence and Security Committee. All our operational processes rigorously support this position.”

These agencies’ refusal to “comment on intelligence matters” – meaning: talk at all about anything and everything they do – is precisely why whistleblowing is so urgent, the journalism that supports it so clearly in the public interest, and the increasingly unhinged attacks by these agencies so easy to understand. Claims that government agencies are infiltrating online communities and engaging in “false flag operations” to discredit targets are often dismissed as conspiracy theories, but these documents leave no doubt they are doing precisely that.

Whatever else is true, no government should be able to engage in these tactics: what justification is there for having government agencies target people – who have been charged with no crime – for reputation-destruction, infiltrate online political communities, and develop techniques for manipulating online discourse? But to allow those actions with no public knowledge or accountability is particularly unjustifiable.

Documents referenced in this article:

- The Art of Deception: Training for a New Generation of Online Covert Operations “

WHEREAS, Defendants are documented by advisors, whistle-blowers and consultants from law enforcement, defense, civil investigation, insider reporters from such as publications as TECH CRUNCH, The Daily Mail, ICIJ, Drudge Report, etc. and intelligence entities as being the persons and parties who did engage in the following attacks on Plaintiffs and said attacks can be tracked back to Defendants via forensic data and said attacks by Defendants threatened the lives, brands, incomes, careers, safety, security, and other metrics of Plaintiffs:

Defendants produced a series of attack videos, articles, blog comments and documents and sent them directly to the spouses, partners, landlords, investors, employers, news media and others in an effort to “vaporize” Plaintiffs as part of the reprisal, vendetta, retribution services which Defendants offered and accepted employment to engage in. Defendants published these attack materials to over 5 billion people for over 5 years in hopes of “destroying” Plaintiffs.

- Defendants contacted Social Security, SSI, SDI, Disability and other earned benefits services and caused them to be stonewalled. Applications were “lost”. Files in the application process “disappeared”. Lois Lerner hard drive “incidents” took place.

Corrupt state and federal employees worked with Defendants to play an endless game of Catch22 by arbitrarily determining that deadlines had passed that they, the government officials, had stonewalled and obfuscated applications for, in order to force these deadlines that they set, to appear to be missed.

Some applicants found themselves strangely poisoned, not unlike the Alexander Litvenko case. Heavy metals and toxic materials were found right after their work with the Department of Energy weapons and energy facilities. Many wonder if these “targets” were intentionally exposed to toxins in retribution for their testimony. The federal MSDS documents clearly show that a number of these people were exposed to deadly compounds and radiations.

Applicants employers were called, and faxed, and ordered to fire applicants from their places of employment, in the middle of the day,with no notice, as a retribution tactic.

Applicants HR and employment records, on recruiting and hiring databases, were embedded with negative keywords and links to Defendants servers in order to prevent them from gaining future employment.

Peers Gary D. Conley and Rajeev Motwani, both whistleblowers in this matter, turned up dead under strange circumstances. They are not alone in a series of bizarre deaths related to this matter.

Paypal, owned by Gawker backer Pierre Omidyar, and other online payments for online sales were delayed, hidden, or redirected in order to terminate income potential for applicants who competed with Defendants interests and holdings.

DNS redirection, website spoofing which sent applicants websites to dead ends and other Internet activity manipulations were conducted.

Campaign finance dirty tricks contractors INQTel, Think Progress, Media Matters, Gawker Media, Syd Blumenthal, etc., were hired and proven to have all been financially connected to Defendants. Executives and their campaign financiers to attack applicants who competed with Defendant executives stocks and personal assets.

Covert Defendant partner: Google, transfered large sums of cash to dirty tricks contractors and then manually locked the media portion of the attacks into the top lines of the top pages of all Google searches globally, for years, with hidden embedded codes in the links and web-pages which multiplied the attacks on applicants by many magnitudes.

Honeytraps and moles were employed by the attackers. In this tactic, people who covertly worked for the attackers were employed to approach the “target” in order to spy on and misdirect the subject. Vanity Fair produced a feature article about one such attack on the Founder of Tech Crunch, a peer.

Mortgage and rental applications had red flags added to them by Defendants in databases to prevent the targets from getting homes or apartments.

McCarthyEra "Blacklists" were created and employed against applicants who competed with Defendants executives and their campaign financiers to prevent them from funding and future employment.

Targets were very carefully placed in a position of not being able to get jobs, unemployment benefits, disability benefits or acquire any possible sources of income. “

The above list is only a partial set of examples of the attacks by Defendants.

WHEREAS, Defendants attacking entities, for whom law enforcement and intelligence surveillance records exist, are, at least, known to include Defendants employees and contractors: Adam Dachis, Adam Weinstein, Adrian Covert, Adrien Chen, Alan Henry, Albert Burneko, Alex Balk, Alexander Pareene, Alexandra Philippides, Allison Wentz, Andrew Collins, Andrew Magary, Andrew Orin, Angelica Alzona, Anna Merlan, Ariana Cohen, Ashley Feinberg, Ava Gyurina, Barry Petchesky, Brendan I. Koerner, Brendan O’Connor, Brent Rose, Brian Hickey, Camila Cabrer, Choire Sicha, Chris Mohney, Clover Hope, Daniel Morgan, David Matthews, Diana Moskovitz, Eleanor Shechet, Elizabeth Spiers, Elizabeth Starkey, Emily Gould, Emily Herzig, Emma Carmichael, Erin Ryan, Ethan Sommer, Eyal Ebel, Gabrielle Bluestone, Gabrielle Darbyshire, Georgina K. Faircloth, Gregory Howard, Hamilton Nolan, Hannah Keyser, Hudson Hongo. Heather Deitrich, Hugo Schwyzer, Hunter Slaton, Ian Fette, Irin Carmon, James J. Cooke, James King, Jennifer Ouellette, Jesse Oxfeld, Jessica Cohen, Jesus Diaz, Jillian Schulz, Joanna Rothkopf, John Cook, John Herrman, Jordan Sargent, Joseph Keenan Trotter, Josh Stein, Julia Allison, Julianne E. Shepherd, Justin Hyde, Kate Dries, Katharine Trendacosta, Katherine Drummond, Kelly Stout, Kerrie Uthoff, Kevin Draper, Lacey Donohue, Lucy Haller, Luke Malone, Madeleine Davies, Madeline Davis, Mario Aguilar, Matt Hardigree, Matt Novak, Michael Ballaban, Michael Dobbs, Michael Spinelli, Neal Ungerleider, Nicholas Aster, Nicholas Denton, Omar Kardoudi, Pierre Omidyar, Owen Thomas, Patrick George, Patrick Laffoon, Patrick Redford, Rich Juzwiak, Richard Blakely, Richard Rushfield, Robert Finger, Robert Sorokanich, Rory Waltzer, Rosa Golijan, Ryan Brown, Ryan Goldberg, Sam Faulkner Bidle, Sam Woolley, Samar Kalaf, Sarah Ramey, Shannon Marie Donnelly, Shep McAllister, Sophie Kleeman, Stephen Totilo, Tamar Winberg, Taryn Schweitzer, Taylor McKnight, Thorin Klosowski, Tim Marchman, Timothy Burke, Tobey Grumet Segal, Tom Ley, Tom Scocca, Veronica de Souza, Wes Siler, William Haisley, William Turton at a minimum but not to be limited by this law enforcement list.

WHEREAS further information provided in the 7 other related federal cases that this Court has been notified of provide further confirming evidence.

WHEREAS financial tracking of the financiers, beneficiaries and means of operations communications prove that a RICO-qualified Cartel was operated by Defendants.

DEMAND IS HEREBY MADE FOR A JOINT DOJ/PLAINTIFF FEDERAL RICO COMPLAINT TO BE FILED AGAINST DEFENDANTS BY DOJ ON BEHALF OF PLAINTIFFS AND THE UNITED STATES TAXPAYERS.

PLEASE TAKE FURTHER NOTICE that copies of any motions scheduled for hearing on the omnibus dates may be obtained free of charge by visiting the website of the Debtors' claims and noticing agent, Prime Clerk LLC, at https://cases.primeclerk.com/gawker.

You may also obtain copies of any pleadings by visiting the Court's website at http://nysb.uscourts.gov in accordance with the procedures and fees set forth therein. You may also obtain copies of non-classified evidence for this case at http://www.globalscoop.net Case # 2788-D in folders # A-1 through A-50.

PROOF OF SERVICE
Plaintiffs group hereby certifies that on this date we caused this filing to be served via a true and correct copy of the foregoing by causing copies of same to be served on all counsel of record, all known creditors, federal law enforcement liaisons and on the U.S. Trustee for the Southern District of New York, Region 2, by electronic filing same via electronically traced and tracked digital networking and using the Prime Clerk case system and the Judge's office electronic filing system.

BCC: FBI, U.S. Congress, FTC, SEC, OSC, GAO, INTERPOL

The last four digits of the taxpayer identification number of the debtors are: Gawker Media LLC (0492); Gawker Media Group, Inc. (3231); and Gawker Hungary Kft. (f/k/a Kinja Kft.) (5056). Gawker Media LLC and Gawker Media Group, Inc.'s mailing addresses are c/o Opportune LLP, Attn: William D. Holden, Chief Restructuring Officer, 10 East 53rd Street, 33rd Floor, New York, NY 10022. Gawker Hungary Kft.'s mailing address is c/o Opportune LLP, Attn: William D. Holden, 10 East 53rd Street, 33rd Floor, New York, NY 10022.