How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations

How the bad guys use Google, Facebook, Twitter and Match.com as weapons against the public



Glenn Greenwald

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:

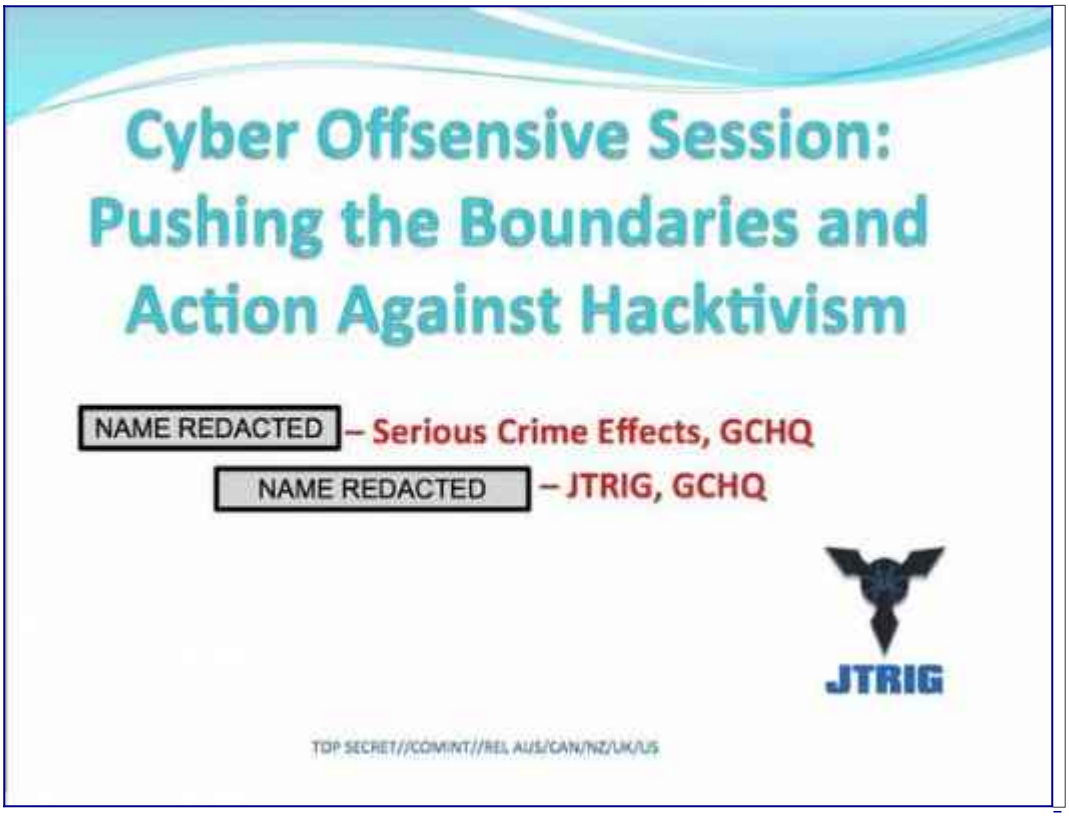


GCHQ describes the purpose of JTRIG in starkly clear terms: “using online techniques to make something happen in the real or cyber world,” including “information ops (influence or disruption).”



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."

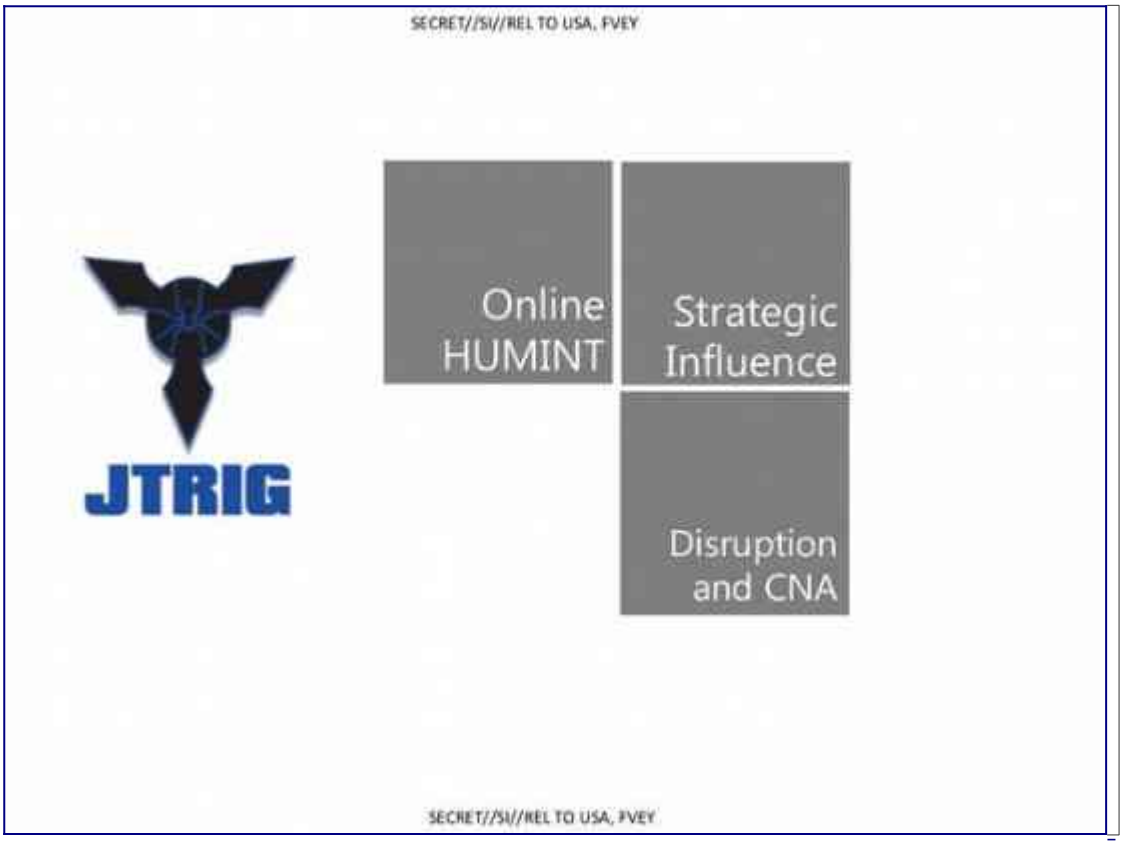
Government plans to monitor and influence internet communications, and covertly infiltrate online communities in order to sow dissension and disseminate false information, have long been the source of speculation. Harvard Law Professor Cass Sunstein, a close Obama adviser and the White House's former 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).

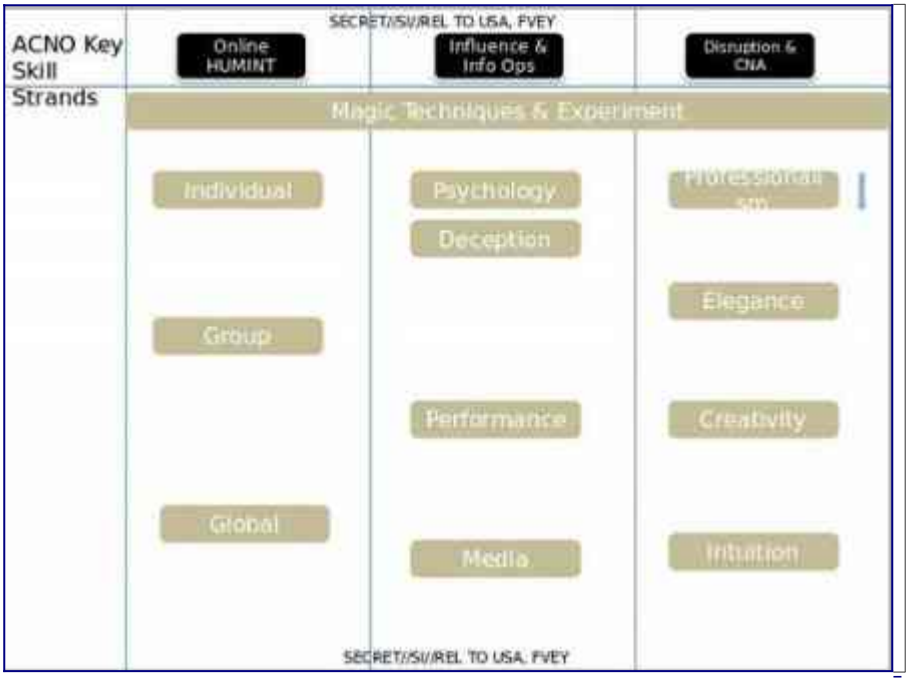
But these GCHQ documents are the first to prove that a major western government is using some of the most controversial techniques to disseminate deception online and harm the reputations of targets. Under the tactics they use, the state is deliberately spreading lies on the internet about whichever 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?

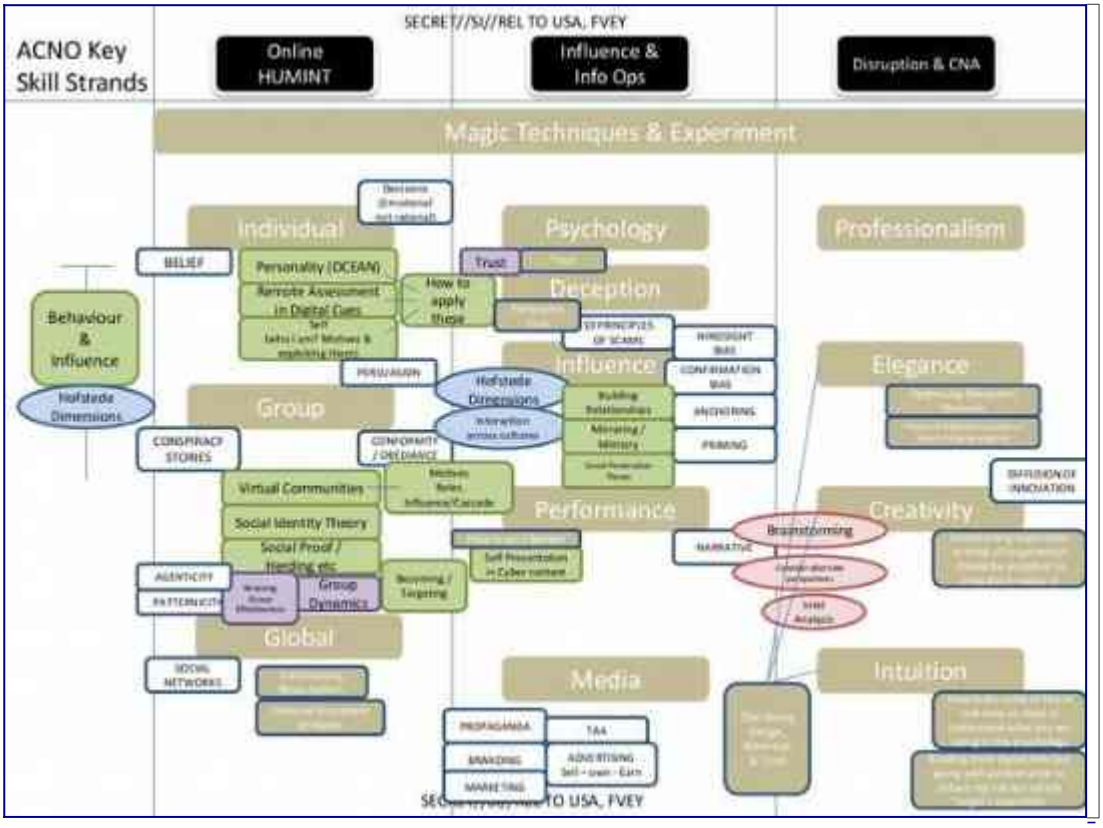
Then there is the use of psychology and other social sciences to not only understand, but shape and control, how online activism and discourse unfolds. Today's newly published document touts the work of GCHQ's "Human Science Operations Cell," devoted to "online human intelligence" and "strategic influence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

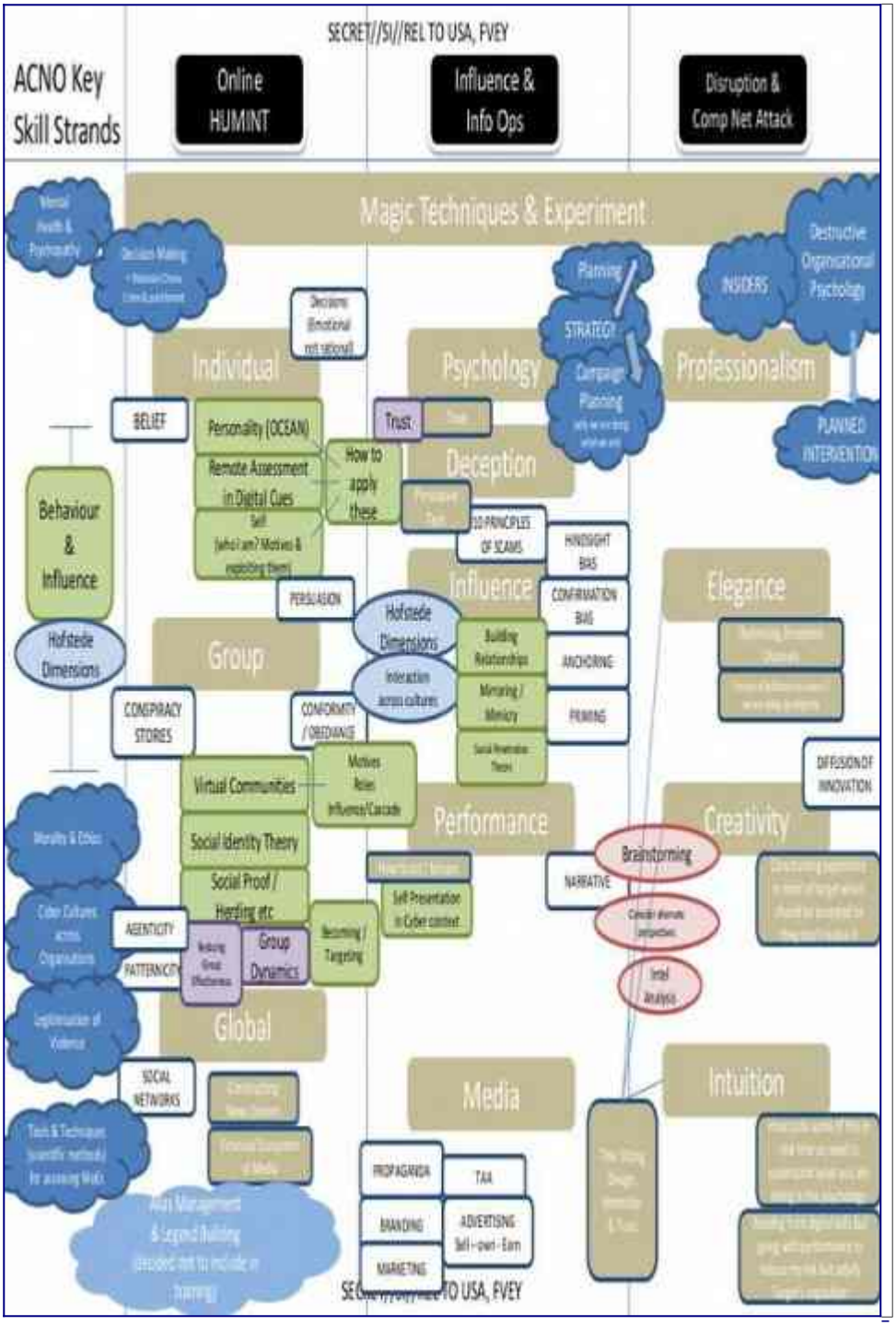


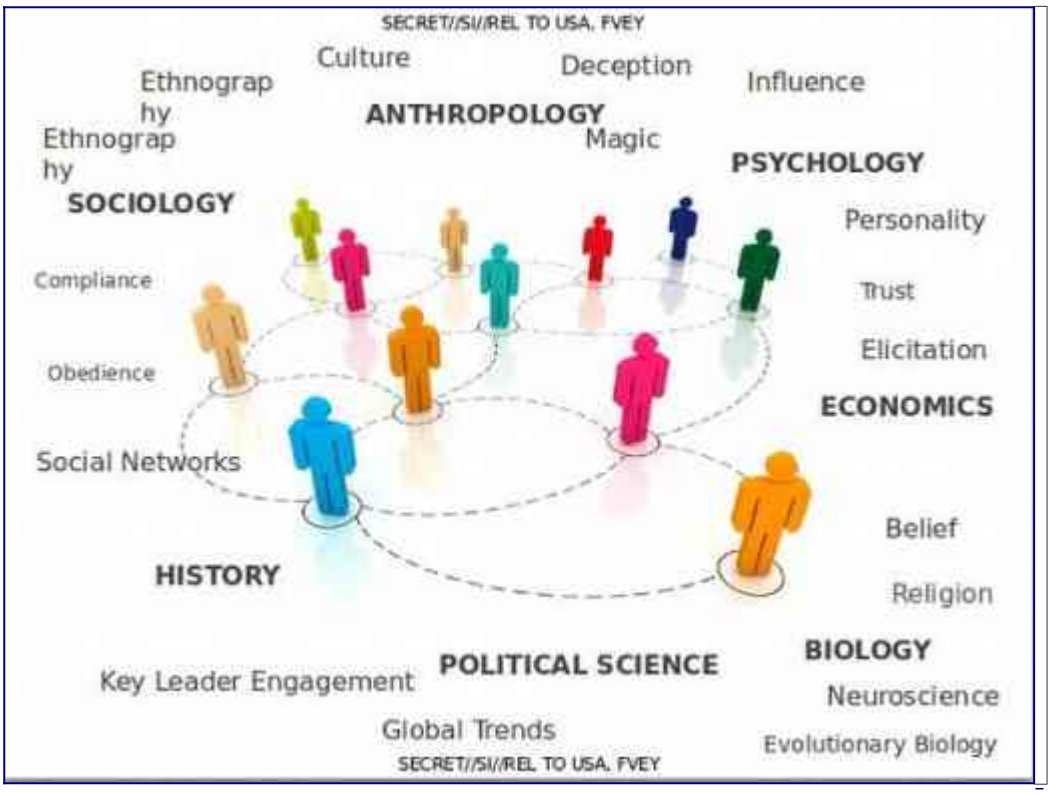


Under the title “Online Covert Action”, the document details a variety of means to engage in “influence and info ops” as well as “disruption and computer net attack,” while dissecting how human beings can be manipulated using “leaders,” “trust,” “obedience” and “compliance”:


SECRET//SI//REL TO USA, FVEY
ACNO Key Skill Strands
Online HUMINT
Influence & Info Ops
Disruption & CNA
Magic Techniques & Experiment
Individual
Psychology
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
How to apply these
Trust
CONSPIRACY STORIES
Virtual Communities
Social Identity Theory
Social Proof / Herding etc
Group Dynamics
AGENTICITY
Brainstorming
NARRATIVE
PRIMING
CONFIRMATION BIAS
ANCHORING
SOCIAL NETWORKS
PROPAGANDA
TAA
BRANDING
ADVERTISING
MARKETING


SECRET//SI//REL TO USA, FVEY
ACNO Key Skill Strands
Online HUMINT
Influence & Info Ops
Disruption & Comp Net Attack
Magic Techniques & Experiment
Individual
Psychology
Professionalism
Deception
Influence
Elegance
Group
Performance
Creativity
Global
Media
Intuition
Behaviour & Influence
BELIEF
Personality (OCEAN)
Remote Assessment in Digital Cues
How to apply these
Trust
Planning
STRATEGY
Campaign Planning
INSIDERS
Destructive Organisational Psychology
PLANNED INTERVENTION
Decisions (Emotional not rational)
Hofstede Dimensions
PERSUASION
Interaction across cultures
Building Relationships
Mirroring / Mimicry
HINDSIGHT BIAS
CONFIRMATION BIAS
ANCHORING
PRIMING
DIFFUSION OF INNOVATION
CONSPIRACY STORIES
CONFORMITY / OBEDIENCE
Virtual Communities
Social Identity Theory
Social Proof / Herding etc
Motives Roles Influence/Cascade
Brainstorming
NARRATIVE
Self Presentation in Cyber context
AGENTICITY
PATTERNICITY
Group Dynamics
Becoming / Targeting
SOCIAL NETWORKS
PROPAGANDA
TAA
BRANDING
ADVERTISING Sell - own - Earn
MARKETING
Asset Management & Legend Building
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:

SECRET//SI//REL TO USA, FVEY

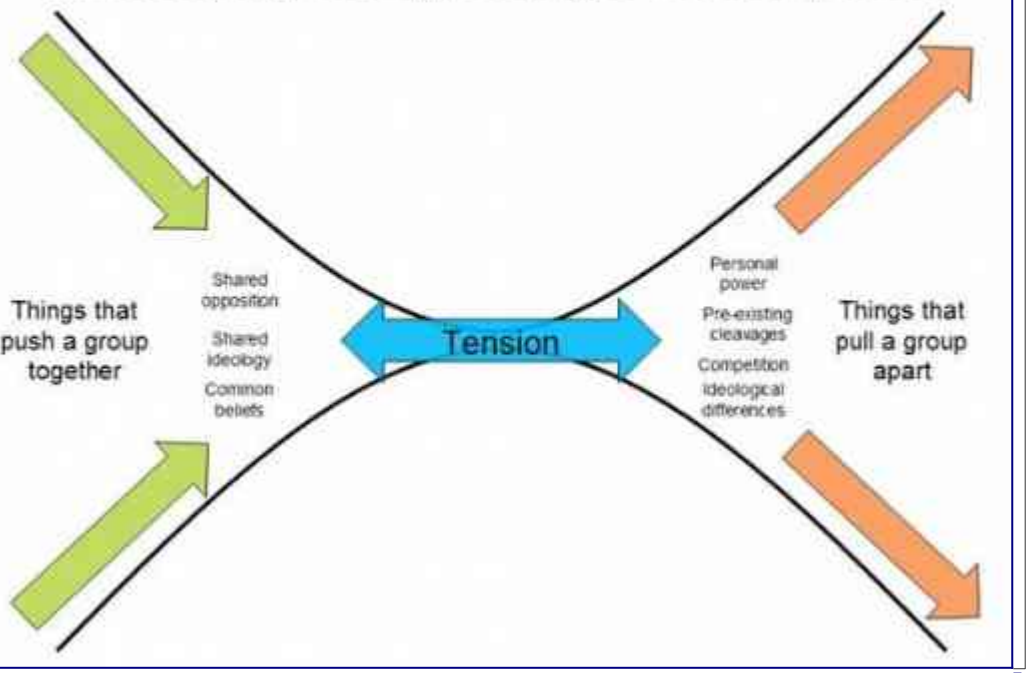
Gambits for Deception

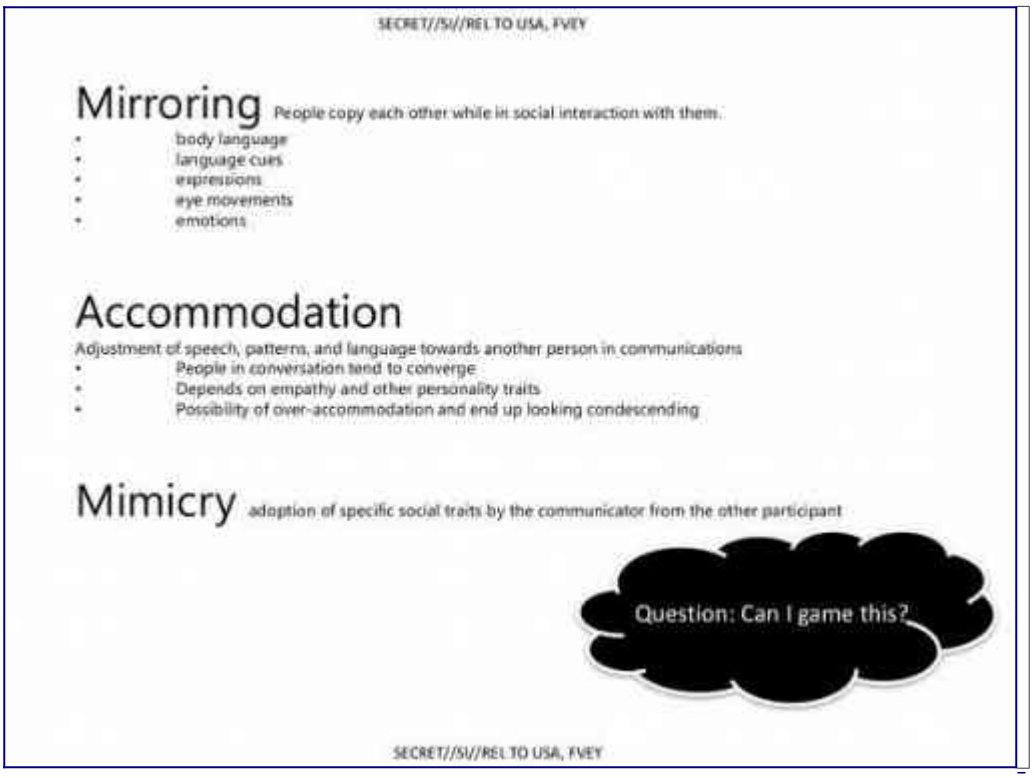
Attention	Control attention Conspicuity & Expectancies	The big move covers the little move	The Target looks where you look	Attention drops at the perceived end	Repetition reduces vigilance
Perception	Mask/Mimic Eliminate - Blend Recreate - Imitate	Repackage/Invent Modify old cues Create new cues	Dazzle/Decoy 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

SECRET//SI//REL TO USA, FVEY

SECRET//SI//REL TO USA, FVEY

Identifying & Exploiting fracture points





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