COINTELPRO Techniques for dilution, misdirection and control of a internet forum. (This valuable information is being scrubbed from the Internet.)
COINTELPRO Techniques for dilution, misdirection and control of a internet forum. There are several techniques for the control and manipulation of a internet forum no matter what, or who is on it. We will go over each technique and demonstrate that only a minimal number of operatives can be used to eventually and effectively gain a control of a 'uncontrolled forum.'

Technique #1 – 'FORUM SLIDING'

If a very sensitive posting of a critical nature has been posted on a forum – it can be quickly removed from public view by 'forum sliding.' In this technique a number of unrelated posts are quietly prepositioned on the forum and allowed to 'age.' Each of these misdirectional forum postings can then be called upon at will to trigger a 'forum slide.' The second requirement is that several fake accounts exist, which can be called upon, to ensure that this technique is not exposed to the public. To trigger a 'forum slide' and 'flush' the critical post out of public view it is simply a matter of logging into each account both real and fake and then 'replying' to prepositined postings with a simple 1 or 2 line comment. This brings the unrelated postings to the top of the forum list, and the critical posting 'slides' down the front page, and quickly out of public view. Although it is difficult or impossible to censor the posting it is now lost in a sea of unrelated and unuseful postings. By this means it becomes effective to keep the readers of the forum reading unrelated and non-issue items.

Technique #2 – 'CONSENSUS CRACKING'

A second highly effective technique (which you can see in operation all the time at www.abovetopsecret.com) is 'consensus cracking.' To develop a consensus crack, the following technique is used. Under the guise of a fake account a posting is made which looks legitimate and is towards the truth is made – but the critical point is that it has a VERY WEAK PREMISE without substantive proof to back the posting. Once this is done then under alternative fake accounts a very strong position in your favour is slowly introduced over the life of the posting. It is IMPERATIVE that both sides are initially presented, so the uninformed reader cannot determine which side is the truth. As postings and replies are made the stronger 'evidence' or disinformation in your favour is slowly 'seeded in.' Thus the uninformed reader will most like develop the same position as you, and if their position is against you their opposition to your posting will be most likely dropped. However in some cases where the forum

members are highly educated and can counter your disinformation with real facts and linked postings, you can then ‘abort’ the consensus cracking by initiating a ‘forum slide.’

Technique #3 – ‘TOPIC DILUTION’

Topic dilution is not only effective in forum sliding it is also very useful in keeping the forum readers on unrelated and non-productive issues. This is a critical and useful technique to cause a ‘RESOURCE BURN.’ By implementing continual and non-related postings that distract and disrupt (trolling) the forum readers they are more effectively stopped from anything of any real productivity. If the intensity of gradual dilution is intense enough, the readers will effectively stop researching and simply slip into a ‘gossip mode.’ In this state they can be more easily misdirected away from facts towards uninformed conjecture and opinion. The less informed they are the more effective and easy it becomes to control the entire group in the direction that you would desire the group to go in. It must be stressed that a proper assessment of the psychological capabilities and levels of education is first determined of the group to determine at what level to ‘drive in the wedge.’ By being too far off topic too quickly it may trigger censorship by a forum moderator.

Technique #4 – ‘INFORMATION COLLECTION’

Information collection is also a very effective method to determine the psychological level of the forum members, and to gather intelligence that can be used against them. In this technique in a light and positive environment a ‘show you mine so me yours’ posting is initiated. From the number of replies and the answers that are provided much statistical information can be gathered. An example is to post your ‘favourite weapon’ and then encourage other members of the forum to showcase what they have. In this matter it can be determined by reverse proration what percentage of the forum community owns a firearm, and or a illegal weapon. This same method can be used by posing as one of the form members and posting your favourite ‘technique of operation.’ From the replies various methods that the group utilizes can be studied and effective methods developed to stop them from their activities.

Technique #5 – ‘ANGER TROLLING’

Statistically, there is always a percentage of the forum posters who are more inclined to violence. In order to determine who these individuals are, it is a requirement to

present a image to the forum to deliberately incite a strong psychological reaction. From this the most violent in the group can be effectively singled out for reverse IP location and possibly local enforcement tracking. To accomplish this only requires posting a link to a video depicting a local police officer massively abusing his power against a very innocent individual. Statistically of the million or so police officers in America there is always one or two being caught abusing there powers and the taping of the activity can be then used for intelligence gathering purposes – without the requirement to 'stage' a fake abuse video. This method is extremely effective, and the more so the more abusive the video can be made to look. Sometimes it is useful to 'lead' the forum by replying to your own posting with your own statement of violent intent, and that you 'do not care what the authorities think!!' inflammation. By doing this and showing no fear it may be more effective in getting the more silent and self-disciplined violent intent members of the forum to slip and post their real intentions. This can be used later in a court of law during prosecution.

Technique #6 – 'GAINING FULL CONTROL'

It is important to also be harvesting and continually maneuvering for a forum moderator position. Once this position is obtained, the forum can then be effectively and quietly controlled by deleting unfavourable postings – and one can eventually steer the forum into complete failure and lack of interest by the general public. This is the 'ultimate victory' as the forum is no longer participated with by the general public and no longer useful in maintaining their freedoms. Depending on the level of control you can obtain, you can deliberately steer a forum into defeat by censoring postings, deleting memberships, flooding, and or accidentally taking the forum offline. By this method the forum can be quickly killed. However it is not always in the interest to kill a forum as it can be converted into a 'honey pot' gathering center to collect and misdirect newcomers and from this point be completely used for your control for your agenda purposes.

CONCLUSION

Remember these techniques are only effective if the forum participants DO NOT KNOW ABOUT THEM. Once they are aware of these techniques the operation can completely fail, and the forum can become uncontrolled. At this point other avenues must be considered such as initiating a false legal precidence to simply have the forum shut down and taken offline. This is not desirable as it then leaves the enforcement agencies unable to track the percentage of those in the population who

always resist attempts for control against them. Many other techniques can be utilized and developed by the individual and as you develop further techniques of infiltration and control it is imperative to share then with HQ.

Twenty-Five Rules of Disinformation.
Note: The first rule and last five (or six, depending on situation) rules are generally not directly within the ability of the traditional disinfo artist to apply. These rules are generally used more directly by those at the leadership, key players, or planning level of the criminal conspiracy or conspiracy to cover up.

Hear no evil, see no evil, speak no evil. Regardless of what you know, don't discuss it — especially if you are a public figure, news anchor, etc. If it's not reported, it didn't happen, and you never have to deal with the issues.

Become incredulous and indignant. Avoid discussing key issues and instead focus on side issues which can be used show the topic as being critical of some otherwise sacrosanct group or theme. This is also known as the 'How dare you!' gambit.

Create rumor mongers. Avoid discussing issues by describing all charges, regardless of venue or evidence, as mere rumors and wild accusations. Other derogatory terms mutually exclusive of truth may work as well. This method which works especially well with a silent press, because the only way the public can learn of the facts are through such 'arguable rumors'. If you can associate the material with the Internet, use this fact to certify it a 'wild rumor' from a 'bunch of kids on the Internet' which can have no basis in fact.

Use a straw man. Find or create a seeming element of your opponent's argument which you can easily knock down to make yourself look good and the opponent to look bad. Either make up an issue you may safely imply exists based on your interpretation of the opponent/opponent arguments/situation, or select the weakest aspect of the weakest charges. Amplify their significance and destroy them in a way which appears to debunk all the charges, real and fabricated alike, while actually avoiding discussion of the real issues.

Sidetrack opponents with name calling and ridicule. This is also known as the primary 'attack the messenger' ploy, though other methods qualify as variants of that approach. Associate opponents with unpopular titles such as 'kooks', 'right-wing', 'liberal', 'left-wing', 'terrorists', 'conspiracy buffs', 'radicals', 'militia', 'racists', 'religious

fanatics', 'sexual deviates', and so forth. This makes others shrink from support out of fear of gaining the same label, and you avoid dealing with issues.

Hit and Run. In any public forum, make a brief attack of your opponent or the opponent position and then scamper off before an answer can be fielded, or simply ignore any answer. This works extremely well in Internet and letters-to-the-editor environments where a steady stream of new identities can be called upon without having to explain criticism, reasoning — simply make an accusation or other attack, never discussing issues, and never answering any subsequent response, for that would dignify the opponent's viewpoint.

Question motives. Twist or amplify any fact which could be taken to imply that the opponent operates out of a hidden personal agenda or other bias. This avoids discussing issues and forces the accuser on the defensive.

Invoke authority. Claim for yourself or associate yourself with authority and present your argument with enough 'jargon' and 'minutia' to illustrate you are 'one who knows', and simply say it isn't so without discussing issues or demonstrating concretely why or citing sources.

Play Dumb. No matter what evidence or logical argument is offered, avoid discussing issues except with denials they have any credibility, make any sense, provide any proof, contain or make a point, have logic, or support a conclusion. Mix well for maximum effect.

Associate opponent charges with old news. A derivative of the straw man — usually, in any large-scale matter of high visibility, someone will make charges early on which can be or were already easily dealt with – a kind of investment for the future should the matter not be so easily contained.) Where it can be foreseen, have your own side raise a straw man issue and have it dealt with early on as part of the initial contingency plans. Subsequent charges, regardless of validity or new ground uncovered, can usually then be associated with the original charge and dismissed as simply being a rehash without need to address current issues — so much the better where the opponent is or was involved with the original source.

Establish and rely upon fall-back positions. Using a minor matter or element of the facts, take the 'high road' and 'confess' with candor that some innocent mistake, in hindsight, was made — but that opponents have seized on the opportunity to blow it

all out of proportion and imply greater criminalities which, ‘just isn’t so.’ Others can reinforce this on your behalf, later, and even publicly ‘call for an end to the nonsense’ because you have already ‘done the right thing.’ Done properly, this can garner sympathy and respect for ‘coming clean’ and ‘owning up’ to your mistakes without addressing more serious issues.

Enigmas have no solution. Drawing upon the overall umbrella of events surrounding the crime and the multitude of players and events, paint the entire affair as too complex to solve. This causes those otherwise following the matter to begin to lose interest more quickly without having to address the actual issues.

Alice in Wonderland Logic. Avoid discussion of the issues by reasoning backwards or with an apparent deductive logic which forbears any actual material fact.

Demand complete solutions. Avoid the issues by requiring opponents to solve the crime at hand completely, a ploy which works best with issues qualifying for rule 10.

Fit the facts to alternate conclusions. This requires creative thinking unless the crime was planned with contingency conclusions in place.

Vanish evidence and witnesses. If it does not exist, it is not fact, and you won’t have to address the issue.

Change the subject. Usually in connection with one of the other ploys listed here, find a way to side-track the discussion with abrasive or controversial comments in hopes of turning attention to a new, more manageable topic. This works especially well with companions who can ‘argue’ with you over the new topic and polarize the discussion arena in order to avoid discussing more key issues.

Emotionalize, Antagonize, and Goad Opponents. If you can’t do anything else, chide and taunt your opponents and draw them into emotional responses which will tend to make them look foolish and overly motivated, and generally render their material somewhat less coherent. Not only will you avoid discussing the issues in the first instance, but even if their emotional response addresses the issue, you can further avoid the issues by then focusing on how ‘sensitive they are to criticism.’

Ignore proof presented, demand impossible proofs. This is perhaps a variant of the ‘play dumb’ rule. Regardless of what material may be presented by an opponent in

public forums, claim the material irrelevant and demand proof that is impossible for the opponent to come by (it may exist, but not be at his disposal, or it may be something which is known to be safely destroyed or withheld, such as a murder weapon.) In order to completely avoid discussing issues, it may be required that you to categorically deny and be critical of media or books as valid sources, deny that witnesses are acceptable, or even deny that statements made by government or other authorities have any meaning or relevance.

False evidence. Whenever possible, introduce new facts or clues designed and manufactured to conflict with opponent presentations — as useful tools to neutralize sensitive issues or impede resolution. This works best when the crime was designed with contingencies for the purpose, and the facts cannot be easily separated from the fabrications.

Call a Grand Jury, Special Prosecutor, or other empowered investigative body. Subvert the (process) to your benefit and effectively neutralize all sensitive issues without open discussion. Once convened, the evidence and testimony are required to be secret when properly handled. For instance, if you own the prosecuting attorney, it can insure a Grand Jury hears no useful evidence and that the evidence is sealed and unavailable to subsequent investigators. Once a favorable verdict is achieved, the matter can be considered officially closed. Usually, this technique is applied to find the guilty innocent, but it can also be used to obtain charges when seeking to frame a victim.

Manufacture a new truth. Create your own expert(s), group(s), author(s), leader(s) or influence existing ones willing to forge new ground via scientific, investigative, or social research or testimony which concludes favorably. In this way, if you must actually address issues, you can do so authoritatively.

Create bigger distractions. If the above does not seem to be working to distract from sensitive issues, or to prevent unwanted media coverage of unstoppable events such as trials, create bigger news stories (or treat them as such) to distract the multitudes.

Silence critics. If the above methods do not prevail, consider removing opponents from circulation by some definitive solution so that the need to address issues is removed entirely. This can be by their death, arrest and detention, blackmail or destruction of their character by release of blackmail information, or merely by destroying them financially, emotionally, or severely damaging their health.

Vanish. If you are a key holder of secrets or otherwise overly illuminated and you think the heat is getting too hot, to avoid the issues, vacate the kitchen.

Eight Traits of the Disinformationalist
1) Avoidance. They never actually discuss issues head-on or provide constructive input, generally avoiding citation of references or credentials. Rather, they merely imply this, that, and the other. Virtually everything about their presentation implies their authority and expert knowledge in the matter without any further justification for credibility.

2) Selectivity. They tend to pick and choose opponents carefully, either applying the hit-and-run approach against mere commentators supportive of opponents, or focusing heavier attacks on key opponents who are known to directly address issues. Should a commentator become argumentative with any success, the focus will shift to include the commentator as well.

3) Coincidental. They tend to surface suddenly and somewhat coincidentally with a new controversial topic with no clear prior record of participation in general discussions in the particular public arena involved. They likewise tend to vanish once the topic is no longer of general concern. They were likely directed or elected to be there for a reason, and vanish with the reason.

4) Teamwork. They tend to operate in self-congratulatory and complementary packs or teams. Of course, this can happen naturally in any public forum, but there will likely be an ongoing pattern of frequent exchanges of this sort where professionals are involved. Sometimes one of the players will infiltrate the opponent camp to become a source for straw man or other tactics designed to dilute opponent presentation strength.

5) Anti-conspiratorial. They almost always have disdain for ‘conspiracy theorists’ and, usually, for those who in any way believe JFK was not killed by LHO. Ask yourself why, if they hold such disdain for conspiracy theorists, do they focus on defending a single topic discussed in a NG focusing on conspiracies? One might think they would either be trying to make fools of everyone on every topic, or simply ignore the group they hold in such disdain.Or, one might more rightly conclude they have an ulterior motive for their actions in going out of their way to focus as they do.

6) Artificial Emotions. An odd kind of ‘artificial’ emotionalism and an unusually thick skin — an ability to persevere and persist even in the face of overwhelming criticism and unacceptance. This likely stems from intelligence community training that, no matter how condemning the evidence, deny everything, and never become emotionally involved or reactive. The net result for a disinfo artist is that emotions can seem artificial.

Most people, if responding in anger, for instance, will express their animosity throughout their rebuttal. But disinfo types usually have trouble maintaining the ‘image’ and are hot and cold with respect to pretended emotions and their usually more calm or unemotional communications style. It’s just a job, and they often seem unable to ‘act their role in character’ as well in a communications medium as they might be able in a real face-to-face conversation/confrontation. You might have outright rage and indignation one moment, ho-hum the next, and more anger later — an emotional yo-yo.

With respect to being thick-skinned, no amount of criticism will deter them from doing their job, and they will generally continue their old disinfo patterns without any adjustments to criticisms of how obvious it is that they play that game — where a more rational individual who truly cares what others think might seek to improve their communications style, substance, and so forth, or simply give up.

7) Inconsistent. There is also a tendency to make mistakes which betray their true self/motives. This may stem from not really knowing their topic, or it may be somewhat ‘freudian’, so to speak, in that perhaps they really root for the side of truth deep within.

I have noted that often, they will simply cite contradictory information which neutralizes itself and the author. For instance, one such player claimed to be a Navy pilot, but blamed his poor communicating skills (spelling, grammar, incoherent style) on having only a grade-school education. I’m not aware of too many Navy pilots who don’t have a college degree. Another claimed no knowledge of a particular topic/situation but later claimed first-hand knowledge of it.

8) Time Constant. Recently discovered, with respect to News Groups, is the response time factor. There are three ways this can be seen to work, especially when the government or other empowered player is involved in a cover up operation:

a) ANY NG posting by a targeted proponent for truth can result in an IMMEDIATE response. The government and other empowered players can afford to pay people to sit there and watch for an opportunity to do some damage. SINCE DISINFO IN A NG ONLY WORKS IF THE READER SEES IT – FAST RESPONSE IS CALLED FOR, or the visitor may be swayed towards truth.

b) When dealing in more direct ways with a disinformationalist, such as email, DELAY IS CALLED FOR – there will usually be a minimum of a 48-72 hour delay. This allows a sit-down team discussion on response strategy for best effect, and even enough time to 'get permission' or instruction from a formal chain of command.

c) In the NG example 1) above, it will often ALSO be seen that bigger guns are drawn and fired after the same 48-72 hours delay – the team approach in play. This is especially true when the targeted truth seeker or their comments are considered more important with respect to potential to reveal truth. Thus, a serious truth sayer will be attacked twice for the same sin.

How to Spot a Spy (Cointelpro Agent)
One way to neutralize a potential activist is to get them to be in a group that does all the wrong things. Why?

The message doesn't get out.

A lot of time is wasted

The activist is frustrated and discouraged

Nothing good is accomplished.

FBI and Police Informers and Infiltrators will infest any group and they have phoney activist organizations established.

Their purpose is to prevent any real movement for justice or eco-peace from developing in this country.

Agents come in small, medium or large. They can be of any ethnic background. They can be male or female.

The actual size of the group or movement being infiltrated is irrelevant. It is the potential the movement has for becoming large which brings on the spies and saboteurs.

This booklet lists tactics agents use to slow things down, foul things up, destroy the movement and keep tabs on activists.

It is the agent's job to keep the activist from quitting such a group, thus keeping him/her under control.

In some situations, to get control, the agent will tell the activist:

"You're dividing the movement."

[Here, I have added the psychological reasons as to WHY this maneuver works to control people]

This invites guilty feelings. Many people can be controlled by guilt. The agents begin relationships with activists behind a well-developed mask of "dedication to the cause." Because of their often declared dedication, (and actions designed to prove this), when they criticize the activist, he or she – being truly dedicated to the movement – becomes convinced that somehow, any issues are THEIR fault. This is because a truly dedicated person tends to believe that everyone has a conscience and that nobody would dissimulate and lie like that "on purpose." It's amazing how far agents can go in manipulating an activist because the activist will constantly make excuses for the agent who regularly declares their dedication to the cause. Even if they do, occasionally, suspect the agent, they will pull the wool over their own eyes by rationalizing: "they did that unconsciously… they didn't really mean it… I can help them by being forgiving and accepting " and so on and so forth.

The agent will tell the activist:

"You're a leader!"

This is designed to enhance the activist's self-esteem. His or her narcissistic admiration of his/her own activist/altruistic intentions increase as he or she identifies with and consciously admires the altruistic declarations of the agent which are deliberately set up to mirror those of the activist.

This is “malignant pseudoidentification.” It is the process by which the agent consciously imitates or simulates a certain behavior to foster the activist’s identification with him/her, thus increasing the activist’s vulnerability to exploitation. The agent will simulate the more subtle self-concepts of the activist.

Activists and those who have altruistic self-concepts are most vulnerable to malignant pseudoidentification especially during work with the agent when the interaction includes matter relating to their competency, autonomy, or knowledge.

The goal of the agent is to increase the activist’s general empathy for the agent through pseudo-identification with the activist’s self-concepts.

The most common example of this is the agent who will compliment the activist for his competency or knowledge or value to the movement. On a more subtle level, the agent will simulate affects and mannerisms of the activist which promotes identification via mirroring and feelings of “twinship”. It is not unheard of for activists, enamored by the perceived helpfulness and competence of a good agent, to find themselves considering ethical violations and perhaps, even illegal behavior, in the service of their agent/handler.

The activist’s “felt quality of perfection” [self-concept] is enhanced, and a strong empathic bond is developed with the agent through his/her imitation and simulation of the victim’s own narcissistic investments. [self-concepts] That is, if the activist knows, deep inside, their own dedication to the cause, they will project that onto the agent who is “mirroring” them.

The activist will be deluded into thinking that the agent shares this feeling of identification and bonding. In an activist/social movement setting, the adversarial roles that activists naturally play vis a vis the establishment/government, fosters ongoing processes of intrapsychic splitting so that “twinship alliances” between activist and agent may render whole sectors or reality testing unavailable to the activist. They literally “lose touch with reality.”

Activists who deny their own narcissistic investments [do not have a good idea of their own self-concepts and that they ARE concepts] and consciously perceive themselves (accurately, as it were) to be “helpers” endowed with a special amount of

altruism are exceedingly vulnerable to the affective (emotional) simulation of the accomplished agent.

Empathy is fostered in the activist through the expression of quite visible affects. The presentation of tearfulness, sadness, longing, fear, remorse, and guilt, may induce in the helper-oriented activist a strong sense of compassion, while unconsciously enhancing the activist's narcissistic investment in self as the embodiment of goodness.

The agent's expresssion of such simulated affects may be quite compelling to the observer and difficult to distinguish from deep emotion.

It can usually be identified by two events, however:

First, the activist who has analyzed his/her own narcissistic roots and is aware of his/her own potential for being "emotionally hooked," will be able to remain cool and unaffected by such emotional outpourings by the agent.

As a result of this unaffected, cool, attitude, the Second event will occur: The agent will recompensate much too quickly following such an affective expression leaving the activist with the impression that "the play has ended, the curtain has fallen," and the imposture, for the moment, has finished. The agent will then move quickly to another activist/victim.

The fact is, the movement doesn't need leaders, it needs MOVERS. "Follow the leader" is a waste of time.

A good agent will want to meet as often as possible. He or she will talk a lot and say little. One can expect an onslaught of long, unresolved discussions.

Some agents take on a pushy, arrogant, or defensive manner:

To disrupt the agenda

To side-track the discussion

To interrupt repeatedly

To feign ignorance

To make an unfounded accusation against a person.

Calling someone a racist, for example. This tactic is used to discredit a person in the eyes of all other group members.

Saboteurs

Some saboteurs pretend to be activists. She or he will ….

Write encyclopedic flyers (in the present day, websites)

Print flyers in English only.

Have demonstrations in places where no one cares.

Solicit funding from rich people instead of grass roots support

Display banners with too many words that are confusing.

Confuse issues.

Make the wrong demands.

Cool Compromise the goal.

Have endless discussions that waste everyone's time. The agent may accompany the endless discussions with drinking, pot smoking or other amusement to slow down the activist's work.

Provocateurs

Want to establish "leaders" to set them up for a fall in order to stop the movement.

Suggest doing foolish, illegal things to get the activists in trouble.

Encourage militancy.

Want to taunt the authorities.

Attempt to make the activist compromise their values.

Attempt to instigate violence. Activisim ought to always be non-violent.

Attempt to provoke revolt among people who are ill-prepared to deal with the reaction of the authorities to such violence.

Informants

Want everyone to sign up and sing in and sign everything.

Ask a lot of questions (gathering data).

Want to know what events the activist is planning to attend.

Attempt to make the activist defend him or herself to identify his or her beliefs, goals, and level of committment.

Recruiting

Legitimate activists do not subject people to hours of persuasive dialog. Their actions, beliefs, and goals speak for themselves.

Groups that DO recruit are missionaries, military, and fake political parties or movements set up by agents.

Surveillance

ALWAYS assume that you are under surveillance.

At this point, if you are NOT under surveillance, you are not a very good activist!

Scare Tactics

They use them.

Such tactics include slander, defamation, threats, getting close to disaffected or minimally committed fellow activists to persuade them (via psychological tactics described above) to turn against the movement and give false testimony against their former compatriots. They will plant illegal substances on the activist and set up an arrest; they will plant false information and set up “exposure,” they will send incriminating letters [emails] in the name of the activist; and more; they will do whatever society will allow.

This booklet in no way covers all the ways agents use to sabotage the lives of sincere an dedicated activists.

If an agent is “exposed,” he or she will be transferred or replaced.

COINTELPRO is still in operation today under a different code name. It is no longer placed on paper where it can be discovered through the freedom of information act.

The FBI counterintelligence program’s stated purpose: To expose, disrupt, misdirect, discredit, and otherwise neutralize individuals who the FBI categorize as opposed to the National Interests. “National Security” means the FBI’s security from the people ever finding out the vicious things it does in violation of people’s civil liberties.

Seventeen Techniques for Truth Suppression
Strong, credible allegations of high-level criminal activity can bring down a government. When the government lacks an effective, fact-based defense, other techniques must be employed. The success of these techniques depends heavily upon a cooperative, compliant press and a mere token opposition party.

Dummy up. If it’s not reported, if it’s not news, it didn’t happen.

Wax indignant. This is also known as the “How dare you?” gambit.

Characterize the charges as “rumors” or, better yet, “wild rumors.” If, in spite of the news blackout, the public is still able to learn about the suspicious facts, it can only be through “rumors.” (If they tend to believe the “rumors” it must be because they are simply “paranoid” or “hysterical.”)

Knock down straw men. Deal only with the weakest aspects of the weakest charges. Even better, create your own straw men. Make up wild rumors (or plant false stories) and give them lead play when you appear to debunk all the charges, real and fanciful alike.

Call the skeptics names like “conspiracy theorist,” “nutcase,” “ranter,” “kook,” “crackpot,” and, of course, “rumor monger.” Be sure, too, to use heavily loaded verbs and adjectives when characterizing their charges and defending the “more reasonable” government and its defenders. You must then carefully avoid fair and open debate with any of the people you have thus maligned. For insurance, set up your own “skeptics” to shoot down.

Impugn motives. Attempt to marginalize the critics by suggesting strongly that they are not really interested in the truth but are simply pursuing a partisan political agenda or are out to make money (compared to over-compensated adherents to the government line who, presumably, are not).

Invoke authority. Here the controlled press and the sham opposition can be very useful.

Dismiss the charges as “old news.”

Come half-clean. This is also known as “confession and avoidance” or “taking the limited hangout route.” This way, you create the impression of candor and honesty while you admit only to relatively harmless, less-than-criminal “mistakes.” This stratagem often requires the embrace of a fall-back position quite different from the one originally taken. With effective damage control, the fall-back position need only be peddled by stooge skeptics to carefully limited markets.

Characterize the crimes as impossibly complex and the truth as ultimately unknowable.

Reason backward, using the deductive method with a vengeance. With thoroughly rigorous deduction, troublesome evidence is irrelevant. E.g. We have a completely free press. If evidence exists that the Vince Foster “suicide” note was forged, they would have reported it. They haven’t reported it so there is no such evidence. Another variation on this theme involves the likelihood of a conspiracy leaker and a press who would report the leak.

Require the skeptics to solve the crime completely. E.g. If Foster was murdered, who did it and why?

Change the subject. This technique includes creating and/or publicizing distractions.

Lightly report incriminating facts, and then make nothing of them. This is sometimes referred to as “bump and run” reporting.

Baldly and brazenly lie. A favorite way of doing this is to attribute the “facts” furnished the public to a plausible-sounding, but anonymous, source.

Expanding further on numbers 4 and 5, have your own stooges “expose” scandals and champion popular causes. Their job is to pre-empt real opponents and to play 99-yard football. A variation is to pay rich people for the job who will pretend to spend their own money.

Flood the Internet with agents. This is the answer to the question, “What could possibly motivate a person to spend hour upon hour on Internet news groups defending the government and/or the press and harassing genuine critics?” Don t the authorities have defenders enough in all the newspapers, magazines, radio, and television? One would think refusing to print critical letters and screening out serious callers or dumping them from radio talk shows would be control enough, but, obviously, it is not.

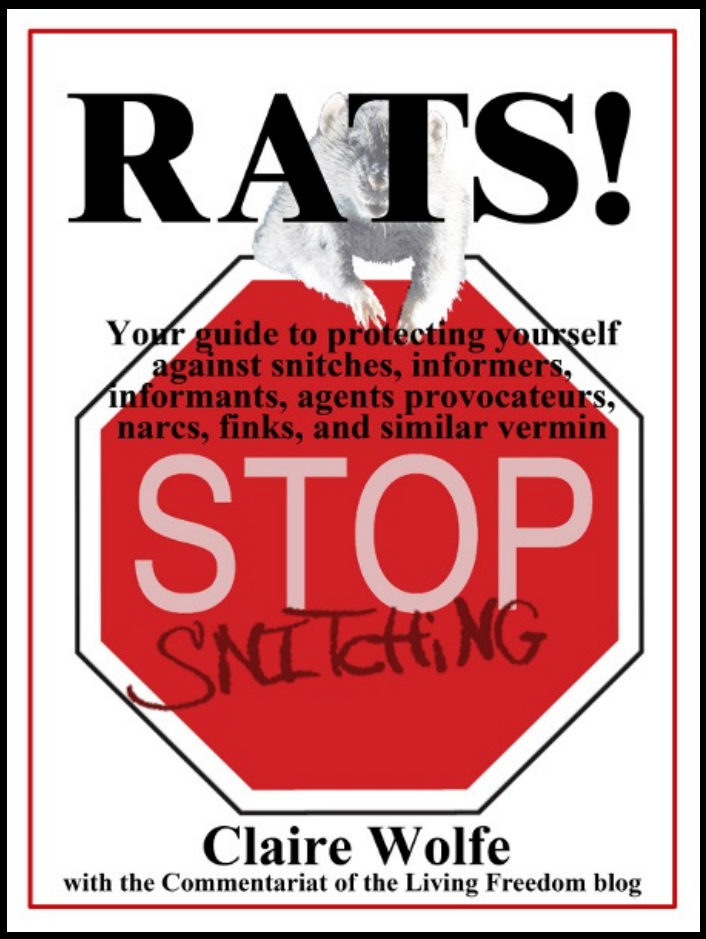
DON'T LET A SNITCH WRECK YOUR LIFE!

This FREE ebook could help keep you out of prison.

Downloads
Kindle (mobi)
Nook (epub)
PDF
Read Online

HTML files
(for hosting on your own site)

Download now by clicking a format in the left column.



These days, law enforcement at all levels -- from the local cop shop to obscure federal agencies -- uses snitches to trap ordinary people. Snitches tell lies that send their friends to jail. Paid agents provocateurs talk or trick otherwise harmless people into committing crimes. In many places, Snitch culture has virtually replaced *real* investigation of *real* crimes.

Don't think you're exempt if you're a "law-abiding citizen." The most trusting, naive, innocent people often make the easiest targets for these weaselly, lying, opportunistic vermin. Snitches specialize in targeting the vulnerable.

You may be in danger if you are:

- A political activist
- A recreational drug user
- A hobbyist or business person who works with "sensitive" materials
- A member of an unpopular religion
- A gun owner or dealer
- A participant in the underground economy
- A photographer or videographer
- A controversial thinker or writer
- Or you just happen to hang out with the wrong people

Snitches are everywhere and they're hard to detect. This brief, FREE ebook, *Rats*, can help you:

- Identify a snitch
- Protect yourself against snitches and agents provocateurs
- Protect your friends or colleagues
- Know how to handle yourself if you get arrested

It could *even help you avoid being pressured into becoming a snitch, yourself*.

Rats is the work of ex-cops, lawyers, security experts, experienced activists, outlaws, former outlaws, trained interrogators, and more. In the hour or so it takes you to read their information, you'll gain a lifetime's worth of armor against snitches, informers, informants, agents provocateurs, narcs, finks, and similar vermin.

Download the *Rats* ebook now. Five electronic formats. **All absolutely FREE. Download below or top of page left.**

Share it with your friends. Spread it around. **Offer copies for download you your own site or mirror this entire page. All we ask is that you provide a link back to http://rats-nosnitch.com/.** Information is power -- the power of free people against a growing police state.

If you want to read the book in one of the ereader formats but don't own a Kindle or a Nook, you can download free reader software for phones, Windows and Mac computers, and other devices. Free Kindle apps from Amazon.com. Free Nook apps from Barnes & Noble.

Downloads

Kindle (mobi)
Nook (epub)
PDF
Read Online

HTML files (for hosting on your own site)

Rats! Your guide to protecting yourself against snitches, informers, informants, agents provocateurs, narcs, finks, and similar vermin
By Claire Wolfe
with the Commentariat of the Living Freedom blog

Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations

Mandeep K. Dhami, PhD
Human Systems Group, Information Management Department, Dstl

10 March 2011

Executive Summary

The importance of influence in cyberspace was highlighted in the recent National Security Strategy and the Strategic Defence and Security Review (UK Government, 2010a, 2010b). JTRIG provides most of GCHQ's cyber effects and online HUMINT capability. It currently lies at the leading edge of cyber influence practice and expertise.

JTRIG targets a range of individual, group and state actors across the globe who pose criminal, security and defence threats. JTRIG staff use a range of techniques to, for example, discredit, disrupt, delay, deny, degrade, and deter. The techniques include: uploading YouTube videos containing persuasive messages; establishing online aliases with Facebook and Twitter accounts, blogs and forum memberships for conducting HUMINT or encouraging discussion on specific issues; sending spoof emails and text messages as well as providing spoof online resources; and setting up spoof trade sites.

Chapter 2 presents the findings of interviewees with a sample of 22 JTRIG staff and seven other staff from GCHQ who support JTRIG's operations. Based on these interviewees, the present report concludes that JTRIG's effects and online HUMINT capability can be further enhanced by providing behavioural science support and improving some of JTRIG's non-technical operational planning and management.

Chapter 3 considers how JTRIG's effects and online HUMINT operations can be grounded in scientific theory and evidence from social psychology (i.e., social cognition, attitudes, persuasive communications, conformity, obedience, interpersonal relationships, trust and distrust, and psychological profiling), including its applications to advertising and marketing, and from criminology (i.e., crime prevention).

Chapter 4 discusses how the effectiveness of JTRIG's effects and online HUMINT operations can be enhanced by improving the current process of assessing the risks associated with conducting operations and the measurement of operational success, and by providing staff with practice/conduct guidelines.

The present report provides the following seven recommendations for supporting and improving JTRIG's effects and online HUMINT capability:

- *Recommendation 1*. JTRIG should train its staff to understand and appropriately apply specific behavioural techniques (see Annexes A to C).

- *Recommendation 2*. Dstl should develop a research programme that: (1) measures the generalisability of specific social influence techniques across cultural groups representative of the types of targets of interest to defence and security organisations so that techniques can be applied appropriately. And, (2) reviews the body of work on influence in cyberspace in order to inform cyber influence operations.

- *Recommendation 3*. Dstl ought to develop a programme of work that assesses the feasibility of compiling psychological profiles based on information available about the individual on the internet so that those conducting online HUMINT operations can compile and exploit such profiles.

- *Recommendation 4*. Dstl ought to develop a programme of work that: (1) reviews the literature identifying the cost-benefit factors motivating individuals to become involved in specific crimes (especially online). And, (2) develops a catalogue of crime prevention techniques that can be applied online.

- *Recommendation 5*. JTRIG should design a *comprehensive* operational risk assessment process.

- *Recommendation 6*. JTRIG should develop a catalogue of measures that provide reliable and valid data on the effectiveness of its online effects and HUMINT operations.

- *Recommendation 7*. JTRIG should develop relevant guidelines describing best practice when conducting operations.

The implementation of recommendations 1 and 5 to 7 require more or less immediate consideration. The implementation of recommendations 2 to 4 refer to delivery of support in the medium- to long-term.

Contents

1. Introduction

1.1 JTRIG provides most of GCHQ's effects capability as well as some of its intelligence capability. JTRIG focuses on the cyber domain (computers and the internet), using both open source data and SIGINT.

1.2 JTRIG's core functions include:

- Covert internet investigations (e.g., researching selectors or targets)
- Forensic investigation and analysis
- Active covert internet operations (including online HUMINT and effects)
- Covert technical operations
- Provision of unattributable internet access
- Development of new (technical) capability

1.3 JTRIG currently comprises approximately 120 staff (excluding integrees) who are organised into three operational groups (i.e., Rest of the World, Counter-Terrorism and Support to Military Operations), and two groups with supporting functions (i.e., Software and Infrastructure Development and Business Oversight).

1.4 The three operational groups can be further sub-divided into teams as follows:

- Rest of the World:
  - Cyber Crime (based in Scarborough)
  - Serious Crime
  - Cyber Co-ordination and Operations
  - Network Defence (based in Bude)
  - Iran
  - Global (non-Iranian targets)
- Counter-Terrorism (CT):
  - Active CT Operations
  - Active Language CT Operations
  - CT Covert Internet Investigations
  - Forensic Analysis
- Support to Military Operations (SMO):
  - Strategic and Tactical Level Effects Delivery
  - Seized Media Exploitation
  - Standby Globally Deployable Capability

1.5 The present report focuses on the work conducted by the above teams (excluding CT Covert Internet Investigations and Forensic Analysis) because they represent JTRIG's online effects and intelligence gathering capability.

1.6 Briefly, the Rest of the World group includes the Iran team that focuses on Iranian targets. The Global team covers any part of the world not covered by other teams (and it currently focuses on the middle-east, Africa, Argentina, Russia, and China). The Serious Crime team covers online drugs and people trafficking (including

illegal immigration) and online financial crime. The Cyber Crime team works on malware, online identity fraud/theft, online child exploitation, domestic extremism, and online credit card fraud/crime. The Cyber Co-ordination and Operations team focuses on individual websites and state cyber attacks. The Network Defence team focuses on malware.

1.7 The CT group focuses on Islamic extremism and Irish Republican extremists. It includes a team of cultural linguists who work in Arabic and who provide cultural and language capability.

1.8 The SMO group consists of both civilian staff and military integrees, and currently focuses on the Afghanistan-Pakistan region. It provides strategic level effects delivery in support of UK and International military partners, tactical support to UK Special Forces in-theatre, analysis of seized media in support of UK facilities in-theatre, and deployable exploitation and effects capability for UK forces.

1.9 Together, the above teams engage in covert internet operations to bring about online HUMINT and effects (defined by GCHQ as “doing things in cyberspace to make something happen”), as well as researching selectors or targets. The work of the teams is supported by some of JTRIG’s other core functions (i.e., covert internet investigations, provision of unattributable internet access, and the development of new technical capability).

1.10 Within GCHQ, the teams work with the relevant Intelligence Production Teams (IPTs) who aid in the initiation and planning of operations based on their analysis of SIGINT, as well as (cultural) linguists (some of whom are native speakers). Several teams currently collaborate with other agencies including the SIS, MoD’s Technical Information Operations (TIO), the FCO, Security Service, SOCA, UK Borders, HMRC, Metropolitan police, and the National Public Order and Intelligence Unit. In addition, the SMO team works closely with 15 Psyops, JIEDAC, the UK military, and Special Forces in-theatre. The nature of collaboration can vary from teams being tasked to perform an effects operation or provide intelligence to them enabling intelligence agencies to make face-to-face contact with a potential source of HUMINT or supporting military operations in-theatre.

1.11 Currently, whereas some of the teams and groups (e.g., Cyber Co-ordination and Operations, Serious Crime, Global, SMO) are primarily tasked to work on specific targets by GCHQ and external organisations and agencies such as SIS, SOCA and Special Forces, other teams (e.g., Cyber Crime, CT) primarily work proactively and opportunistically in searching for targets. However, all teams are responsive to external tasking. Those who task JTRIG are asked to specify the expected outcome of an operation, and provide relevant background information.

1.12 Depending on the prioritisation of the task, JTRIG can respond to requirements for operations on a timescale from a few hours, and operations can be long-term. Operations are not limited to commercial working hours. Importantly, JTRIG’s work is bounded by legal and policy requirements, and all effects operations are subject to approval by Operational Management Groups (OMGs).

Goals and Method of Present Report

1.13 The main goal of the present report is to provide an assessment of JTRIG's behavioural science support requirements for conducting effects and online HUMINT operations. Given that such support would need to occur within certain bounds, a secondary goal is to provide an assessment of some of JTRIG's other (non-technical) operational planning and management requirements such as risk assessment and conduct guidelines.

1.14 These two goals were achieved by a combination of data collection from a sample of JTRIG staff and other staff from GCHQ supporting JTRIG's operations, and a brief review of the relevant behavioural science literature. Data collection involved face-to-face interviews with 29 individuals. Six were interviewed in pairs and the rest were interviewed individually. Interviews lasted approximately one hour (range = 45 minutes to two hours).

1.15 Of the 29 interviewees, 22 were staff representing each of the teams in JTRIG's three operational groups. Seven were staff from elsewhere within GCHQ who support JTRIG's operations (i.e., three staff from the IPTs working with the Iran and serious crime teams, one native language speaker (cultural linguist) working with the Iran team, two OMG chairs, and one legal advisor.

1.16 Interviewees from JTRIG's three operational groups were asked to comment on the following:

- Examples of effects and online HUMINT operations
  - Targets
  - Goals
  - Methods/techniques
- Operational planning and management
  - Risk assessment
  - Measures of effectiveness/success of operations
- Staff development
  - Past work experience
  - Behavioural science needs (if any)

1.17 Interviewees from outside of JTRIG (i.e., GCHQ) were asked to comment broadly on how they support the JTRIG teams, and how behavioural science input could (if at all) support their own work as well as JTRIG's operations.

2. Overview of JTRIG's Effects and Online HUMINT Operations

2.1 The present chapter provides a summary of the data gathered from the interviews of a sample of JTRIG staff and staff from GCHQ who support JTRIG's effects and online HUMINT operations. Given the main goal of the present report, only those issues pertaining to *influence* will be presented here.

Examples of Effects and Online HUMINT Operations

2.2 *Operation targets.* JTRIG's operations may cover all areas of the globe. Staff described operations that are currently targeted at, for example, Iran, Africa, Argentina, Afghanistan, Pakistan, North Korea, UK, and Eastern Europe, including Russia. Operations may target specific individuals (e.g., suspect caught in-theatre or cyber criminal), groups (e.g., Islamic extremists or those engaged in online credit card fraud), the general population (e.g., Iranians), or regimes (e.g., Zanu PF).

2.3 *Operation aims*. Staff noted that the overall goals of an operation and the general content of a communication/message may be dictated by Government policy. Generally, the language of JTRIG's operations is characterised by terms such as "discredit", promote "distrust," "dissuade", "deceive", "disrupt", "delay", "deny", "denigrate/degrade", and "deter."

2.4 According to staff, the Iran team currently aims to achieve counter-proliferation by: (1) discrediting the Iranian leadership and it's nuclear programme; (2) delaying and disrupting access to materials used in the nuclear programme; (3) conducting online HUMINT; and (4) counter-censorship. The Serious Crime team currently aims to reduce online organised crime by: (1) disrupting the activities of front companies; and (2) discrediting the online presence of such companies and their owners as well as promoting distrust among them and consumers. Two of the Global team's current aims are regime change in Zimbabwe by discrediting the present regime, and preventing Argentina from taking over the Falkland Islands by conducting online HUMINT. The CT group's operations currently aim to counter Islamic radicalisation and monitor Irish Republican dissident groups by: (1) disrupting the dissemination of extremist material over the internet; (2) discrediting extremist sites and individuals/groups; (3) conducting online HUMINT; and (4) hosting extremist sites (to enable collection of SIGINT). The Cyber Coordination and Operations team currently aims to investigate cybercrime and electronic attack by: (1) denying, deterring or dissuading criminals, state actors and hacktivists; (2) providing intelligence for judicial outcomes; and (3) discrediting cybercrime forums and their users. The team also acts as a liaison and support for JTRIG teams in Bude and Scarborough. The Network Defence team currently aims to safeguard critical computer networks against cyberattack by: (1) discrediting cybercriminals and malware providers; (2) disrupting State sponsored malware infrastructure; and (2) conducting online HUMINT. Two of the Cyber Crime team's current aims are to prevent and reduce

online credit card fraud and child exploitation by: (1) disrupting the dissemination of child porn, malware and data gathered by it; (2) discrediting those selling stolen credit card and ID details or child porn online and promoting distrust in them; (3) deterring, disrupting or degrading online consumerism of stolen data or child porn; and (4) increasing the reporting of online crime. The Cyber Crime team's other current aim is to monitor domestic extremist groups such as the English Defence League by conducting online HUMINT. Finally, some of the SMO group's current aims are counter-insurgency including counter-improvised explosive device by: (1) denying and disrupting the Taliban message; (2) strategic messaging; (3) delivering tactical in-theatre effects supporting Special Forces; and (4) seized media exploitation.

2.5 *Operation methods/techniques*. All of JTRIG's operations are conducted using cyber technology. Staff described a range of methods/techniques that have been used to-date for conducting effects operations. These included:

- Uploading YouTube videos containing "persuasive" communications (to discredit, promote distrust, dissuade, deter, delay or disrupt)
- Setting up Facebook groups, forums, blogs and Twitter accounts that encourage and monitor discussion on a topic (to discredit, promote distrust, dissuade, deter, delay or disrupt)
- Establishing online aliases/personalities who support the communications or messages in YouTube videos, Facebook groups, forums, blogs etc
- Establishing online aliases/personalities who support other aliases
- Sending spoof e-mails and text messages from a fake person or mimicking a real person (to discredit, promote distrust, dissuade, deceive, deter, delay or disrupt)
- Providing spoof online resources such as magazines and books that provide inaccurate information (to disrupt, delay, deceive, discredit, promote distrust, dissuade, deter or denigrate/degrade)
- Providing online access to uncensored material (to disrupt)
- Sending instant messages to specific individuals giving them instructions for accessing uncensored websites
- Setting up spoof trade sites (or sellers) that may take a customer's money and/or send customers degraded or spoof products (to deny, disrupt, degrade/denigrate, delay, deceive, discredit, dissuade or deter)
- Interrupting (i.e., filtering, deleting, creating or modifying) communications between real customers and traders (to deny, disrupt, delay, deceive, dissuade or deter)
- Taking over control of online websites (to deny, disrupt, discredit or delay)
- Denial of telephone and computer service (to deny, delay or disrupt)
- Hosting targets' online communications/websites for collecting SIGINT (to disrupt, delay, deter or deny)
- Contacting host websites asking them to remove material (to deny, disrupt, delay, dissuade or deter)

2.6 Some of JTRIG's staff have conducted online HUMINT operations. Such operations typically involve establishing an online alias/personality who has a Facebook page, and membership of relevant web forums, etc. The target is then

befriended (or the target befriends the alias). Interactions with the target may be informed by a combination of analysis of SIGINT provided by the IPTs, monitoring of the target's online behaviour, and intelligence from SIS "on-the-ground". The goal may be to collect intelligence and/or to facilitate SIS contact in order to disrupt, delay, deceive, deter or dissuade.

JTRIG Staff Views of Operational Planning and Management

2.7 *Risk assessment*. For the most part, staff noted that risk assessments for operations were conducted by the individual(s) planning and leading the operation. Sometimes risk assessments were done by the agency that was tasking or collaborating with them on an operation (e.g., Security Services).

2.8 A risk assessment typically referred to identification of the potential costs (drawbacks) and/or an estimation of the likelihood of the costs occurring. Commonly identified costs included:

- Being discovered (i.e., as a GCHQ operation)
- Loss of credibility or trust or confidence of target
- Being blocked from the website, internet or telephone service
- Incitement
- Entrapment
- Aiding and abetting (or providing cyber criminals new ideas)
- Physical harm to the target (either from others or themselves)
- Displacement so that target moves to other sites or regions
- Target changes/adapts tactic (e.g., uses middle-men)
- Threatening a target's ego could lead to a counter effect
- The influence communication may interact with an existing message to create an unexpected adverse effect
- Damaging international relations between the target country and the country to which the online communication can be attributed
- Interfering/confounding operations being conducted by other agencies (who may sometimes represent other countries)
- Wasted time due to failure to deconflict with another agency that is also occupying the same cyberspace and/or conducting an (on- or off-line) operation
- Financial cost

2.9 Staff noted that the magnitude and likelihood of the risks (costs) may differ according to the target of the operation. For example, the risk of being discovered conducting operations against a regime are greater in some countries (e.g., China) than others (e.g., Africa), and the risk is considerably less when the operation is conducted against an individual or group than against a regime.

2.10 Staff also noted that some risks could be reduced. For example, the risk of being discovered or for misattribution of the operation to a specific state, group or individual could be reduced by creating a spoof alias/personality or group who overtly

takes responsibility for the "attack." Staff in larger teams (e.g., CT) routinely shared alias details in order to deconflict with one another.

2.11 *Measures of effectiveness/success of operations*. Overall, staff considered that it was difficult to measure operational success, although it was easier for operations with certain types of goals (e.g., deny or denigrate/degrade). They described little routine, formal measurement of the effectiveness/success of the operations that they had conducted. However, discussion led to the identification of several potential variables that could be measured as well as the methods that could be used to measure them. These included:

- Count the number and/or location of views (e.g., for YouTube video) or hits to a website to see if people have accessed the message
- Check online and/or collect SIGINT to see if a message has been attended to, understood, accepted, remembered, and changed behaviour (e.g., people have spread the message and communicate support for it, people lack trust in the discredited individual/group/regime, people are delayed or deterred from an activity or interaction)
- Count the number and significance of friends that an alias has, people who have joined the Facebook group, people who have responded to a blog, or customers who have viewed a trade site (or seller)
- Count the amount of money that customers spend in spoof trade sites (or with sellers)
- Measure the amount of time that customers spend engaging with spoof trade sites (or sellers)
- Count the amount of money that is saved by removing stolen IDs from the internet
- Analyse the content of communication between a potential source of online HUMINT and the alias to see if he/she is providing useful intelligence
- Count the number of times a potential source of online HUMINT initiates communication with the alias
- Check if a potential source of online HUMINT does meet with the SIS as intended
- Check online and/or collect SIGINT to see if people have accessed uncensored material that has been made available to them
- Check online to see if hosts who have been asked to delete material have done so
- Count the number of websites taken down
- Count the number of illegal material (e.g., child porn photos or stolen credit cards removed from a website)
- Check if an individual or group does allow their site to be hosted (unknowingly) by JTRIG
- Count the number of people arrested for a specific offence whom JTRIG has identified

2.12 Most of the above measures of operational success are quantitative. Some are only indirectly indicative of the operational aim being achieved. And, there was little consideration of the durability of the effects. It is also clear that measurement of operational success may require support from other areas of GCHQ (e.g., to obtain

SIGINT) as well as external agencies such as SIS (e.g., to assess the usefulness of online HUMINT).

2.13 Staff suggested that the success of an operation may be threatened by factors such as the:

- Lack of continuity in maintaining an alias or communicating via an alias if a staff member is away and his/her work is covered by others
- Difficulty in maintaining more than a small number (e.g., 2 or 3) of unique, multi-dimensional, active aliases, especially when doing online HUMINT
- Difficulty of communicating in a fashion representative of the socio-cultural-demographic category of an alias
- Lack of photographs/visual images of online aliases
- Lack of time and staff to maintain blogs and aliases, and search for extremist material on the web etc
- Lack of sufficient number and varied cultural language advisors e.g., Russian, Arabic, Pashtu
- Distractions from the JTRIG floor plate/office environment when communicating with targets
- Lack of co-ordination/understanding of the FCO or HMG's changing policies, (and with ISAF or MoD – a potential problem for the SMO team)
- Suspicion aroused by the fact that staff cannot meet face-to-face with targets who are geographically close
- Suspicion aroused by the fact that staff cannot communicate on instant messenger with those speaking a different language

2.14 Staff also noted that in some cases efforts had already been made to reduce the threats to operational success. For instance, in order to increase continuity in maintaining an alias or communicating via an alias when covering for a member of staff who is away, records of past communications were taken (although these were time consuming to read and did not clearly highlight the nonverbal aspects of the online communication e.g., use of grammar). In one case, a staff member "shadowed" another before he left in order to facilitate a smooth transition in taking over an alias.

2.15 Finally, despite a lack of consistent and comprehensive approach to measuring operational success, staff recognised the potential usefulness of measuring the success of operations. For example, there is a need to understand if successful operations generalise to different cultures (e.g., Western versus Eastern, business versus customer, and opportunistic versus professional offenders).

Staff Development

2.16 *Background and experience*. The background and work experience of JTRIG staff includes IT, computing, politics, languages, law, maths, chemistry, sociology, journalism, publishing, police, and military/defence. Many of the staff have worked in other areas of GCHQ before coming to JTRIG. Therefore, although staff have a

range of potentially useful and relevant experiences and varied backgrounds, there is a gap in their formal knowledge of the human/behavioural sciences.

2.17 Staff said they had essentially trained themselves "on-the-job" or learned from observing/shadowing more experienced staff, although some noted they had gone on external training courses. In some cases, staff felt they were sometimes reliant on others and lacked some confidence. Some staff were also concerned about the morality and ethics of their operational work, particularly given the level of deception involved.

2.18 *Behavioural science needs*. Staff identified various areas of behavioural science support that their effects and online HUMINT operations might benefit from. These mostly referred to social psychology, and included:

- Psychology of relationships (including online social interactions)
- Cultural impact on social interactions
- Psychology of trust and distrust
- Psychological profiling
- Developing realistic online aliases/personalities
- Psychology of persuasion
- Mass messaging
- Marketing/branding of YouTube videos
- Plausible excuses for not being able to communicate or interact with target online (or face-to-face)
- Effective delay tactics and "hooks" when dealing with online customers
- Online criminal behaviour (e.g., child exploitation, fraud)
- Youth behaviour online
- Online business operations

2.19 In addition, staff said they needed more information on the following:

- Awareness of current affairs (relevant to a specific region or group) to ensure the message is relevant (in time and place)
- Relevant subject matter expertise
- Awareness of legalities of operational work
- Practice using social networking sites
- Language training

Views of Others Supporting JTRIG

2.20 Interviewees from outside of JTRIG were asked to comment broadly on how they support the JTRIG teams, and how behavioural science input could (if at all) support their work.

2.21 *IPTs*. The IPTs are the operation managers and have target expertise and domain knowledge. They decide on the most appropriate message that needs to be communicated in order to influence. They provide SIGINT useful for understanding the target such as his/her behaviours, relationships, interactions, and online

presence. Currently, IPTs rely on commonsense and cultural experience. IPTs would find behavioural science useful to help them ascertain a target's motivations in order to plan effective operations.

2.22 *Cultural linguists*. JTRIG is reliant on GCHQ's Central Language Team and linguists in IPTs, but does have its own Arabic language capability (mainly in the CT group). Linguists help to write and revise communications so they are linguistically accessible and culturally appropriate; suggest online locations where messages can be best posted; and maintain online aliases for blogging etc. Linguistic support, however, does not overcome the fact that language barriers limit the use of instant messaging when conducting online HUMINT. The fact that linguists (like others) cannot see the target, leads them to try to "guess" how best to interact with the target and how to interpret the target's reactions. They familiarise themselves with the websites and issues being discussed in order to inform their own online interactions via blogs etc. Linguists would find behavioural science useful in knowing how to attract an audience to their blogs and/or make online friends.

2.23 *Legal advisors*. The legal advisors ensure that operations comply with laws, and this may result in operations being revised or blocked. The process involves: (1) deciding whether the operation fulfils one of GCHQ's statue functions, and whether it is necessary and proportionate; (2) identifying if the operation complies with any applicable UK law, and if it doesn't then obtaining authorisation from the Secretary of State; and (3) identifying if the operation complies with any applicable international law, and if it doesn't considering whether non-compliance would be acceptable among the 5-eyes community. However, it is difficult to apply the principles of necessity and proportionality if operational plans are imprecise and partial. In addition, whereas legal compliance is more straightforward, policy compliance is difficult to ascertain, and consideration of ethical compliance is even more difficult. JTRIG staff (especially those leading operations) are provided mandatory legality training. Nevertheless, it might be useful for JTRIG staff to know more about these issues.

2.24 *OMGs*. The OMGs provide governance and oversight of operations, and they comprise relevant members of the IPT, JTRIG staff, policy, and legal advisors. Currently, when requesting OMG approval for an operation, the operation lead is expected to provide the following information: A brief description of the operation (including aim and method); assessment of the risks involved (e.g., risks to individuals, accessibility/visibility to a hostile SIGINT agency, attribution to the UK or HMG, and risk to existing US/UK accesses); target; techniques to be used; legal position and authorisation; policy constraints; and additional operational constraints. It may also be useful to provide information on: The rationale for the operation (e.g., business case); the risks to ongoing operations/investigations and the need to deconflict; how risks could be mitigated; the resources needed for the operation (e.g., human, financial, practical/technical, other agencies); and a prediction of the outcomes of the operation. All of the above information could be elicited using a "why, what, when, where, how (and why)" approach. This may make the OMG process more consistent and transparent, and increase the likelihood that all of the information needed by external partners is available. The OMG considers if an operation complies with legal, political and practical concerns. However, concepts

such as “proportionality” and “necessity” are undefined and open to subjective interpretation. OMGs may also find it difficult to assess the operation if its goals are unclear. Currently, there are no specific guidelines on ethical practice. Risk is calculated in terms of likelihood and impact of costs, and refers mostly to technical, operational and legal/policy factors. The approach to risk assessment is based on qualitative discussion rather than quantitative scientific/statistical methods. Although JTRIG does some Battle Damage Assessment (BDA) after an operation, precise measures of success would be useful for OMGs considering whether resource and cost intensive operations should proceed. More information on operational success might also reduce any risk aversion among OMGs (especially for more ethically complex operations).

3. Behavioural Science Support

3.1 Given the goals and (individual/group) targets of JTRIG's operations, there are various ways in which knowledge gleaned from the behavioural sciences can be used to inform the methods/techniques that JTRIG currently uses for it's effects and online HUMINT operations as well as help JTRIG to develop new ones. Specifically, JTRIG's operations can benefit from psychologically grounded influence techniques and psycho-criminological approaches to influencing prevention. This chapter provides a brief description of some of these techniques and approaches (it is necessarily illustrative rather than exhaustive; see also Annex A).

Psychology-Based Influence Techniques

3.2 Theories and research in the field of social psychology may prove particularly useful for informing JTRIG's effects and online HUMINT operations. The following topics would be particularly relevant for *social influence*:

- Social cognition (including social perception and attribution)
- Attitudes
- Persuasive communications
- Conformity
- Obedience
- Interpersonal relationships
- Trust and distrust
- Psychological profiling

In addition, the application of social psychological ideas to marketing and advertising would be useful. A brief synopsis of the most relevant aspects of each of these topics is provided below (see also Bachmann & Zaheer, 2008; Cialdini, 2009; Fiske, 2010; Fiske, Gilbert, & Lindzey, 2010; Forgas, Copper, & Crano, 2010; Hogg & Vaughan, 2008; Horowitz & Strack, 2010; Maio & Haddock, 2009).

3.3 *Social cognition* refers to how we perceive aspects of our social world, including other people, ourselves and social situations. Impression management or self-presentation can be used to influence how others perceive us. This can be achieved via several different techniques including: Matching others' behaviour; conforming to situational norms; ingratiation; consistency of self; self-promotion; credible intimidation; exemplary behaviour; and supplication (i.e., needing help). The ability to see how others view us and to self-monitor so we can adapt our self-presentation to the situation, are important skills to possess for effective impression management.

3.4 *Attitudes* reflect a combination of beliefs and values that partly affect how we think, feel and behave. People may change their attitudes in order to achieve a sense of internal consistency – in fact, they may selectively attend to and interpret information that increases such dissonance, especially when it arises out of a

voluntary decision or action (and if this was attributed to an internal rather than external state). When specific attitudes are important to an individual, attitude change may only occur after systematic processing of the content of a persuasive communication. By contrast, when an attitude is not personally involving then attitude change may occur through heuristic processing of the content of the communication, and people may be persuaded by peripheral or even non-relevant information. Attitude formation or change based on heuristic processing may be more unreliable and so less predictive of behaviour and also easier to alter. Attitude change may be induced by fear or vulnerability to threat. However, high levels of fear may inhibit change if people lack confidence or knowledge of how to reduce the threat to them. Attitudes (especially prejudicial ones) that have an ego-defence function can be more resistant to change. Prejudicial attitudes may be reduced by increasing contact with the person or object against which the prejudice is directed (Pettigrew & Tropp, 2006). Crucially, this contact should be of equal status and in a cooperative context, frequent, not anxiety or threat inducing, and encouraging positive cross-group relations.

3.5 *Persuasive communications* should focus on the communicator, message, recipient, and the situation. Effective communication campaigns should ask the following: What is the credibility, status, attractiveness, and trustworthiness of the source? Is the message explicit or implicit, emotional or informational, one- or two-sided, and in what order is it presented relative to other information (i.e., first or last)? What is the education level of the recipient, what functions does the attitude have, how resistant is that person to persuasion, and willing to accept or reject the message? Finally, is the situation formal or informal? Messages that are specific are more likely to be effective. In order to persuade, the recipient needs to have access to the message, to have attended to it, understood it, and accepted it, remembered it, and behaved according to it. *Propaganda* techniques include: Using stereotypes; substituting names/labels for neutral ones; censorship or systematic selection of information; repetition; assertions without arguments; and presenting a message for and against a subject.

3.6 *Obedience* is a direct form of social influence where an individual submits to, or complies with, an authority figure. Obedience may be explained by factors such as diffusion of responsibility, perception of the authority figure being legitimate, and socialisation (including social role). Compliance can be achieved through various techniques including: Engaging the norm of reciprocity; engendering liking (e.g., via ingratiation or attractiveness); stressing the importance of social validation (e.g., via highlighting that others have also complied); instilling a sense of scarcity or secrecy; getting the “foot-in-the-door” (i.e., getting compliance to a small request/issue first); and applying the “door-in-the-face” or “low-ball” tactics (i.e., asking for compliance on a large request/issue first and having hidden aspects to a request/issue that someone has already complied with, respectively). Conversely, efforts to reduce obedience may be effectively based around educating people about the adverse consequences of compliance; encouraging them to question authority; and exposing them to examples of disobedience.

3.7 *Conformity* is an indirect form of social influence whereby an individual’s beliefs, feelings and behaviours yield to those (norms) of a social group to which the

individual belongs or to a reference group. Conformity may reflect a person being converted (internalising) or simply being publically compliant. Conformity may be explained by the need to have an accurate representation of the world (via social comparison) and to be accepted by others (by adhering to a norm). Typically, minorities may conform to majorities. However, minority groups can influence the majority by showing a sense of consistency; demonstrated investment; independence; balanced judgment; and similarity to the majority in terms of age, gender and social category.

3.8 The psychology of *interpersonal relationships* focuses on how relationships begin, are maintained and disintegrate. People are more likely to seek affiliation (others' company) when feeling anxious, having experienced a relationship breakdown, or in a new environmental setting. Here, people seek those who have had similar experiences as them (for, e.g., social comparison and information purposes). Indeed, similarity of sociological, demographic and psychological variables is important in enduring relationships. Interpersonal relationships may begin through the reward value of factors such as proximity; exposure; familiarity; similarity; and physical attractiveness. Reciprocal self-disclosure is an important step in the process of developing a relationship. As social exchanges, reciprocal relationships are rewarding. However, relationships in western and non-western cultures differ in terms of, for example, their individualistic-collectivist, voluntary-involuntary, and temporary-permanent nature. Self-disclosure can be increased via reciprocity, situational norms, trust, and the intimacy of a relationship. Women are likely to disclose more than men.

3.9 *Trust* is characterised as involving levels of hope, faith, confidence, passivity and hesitance (Lewicki, McAllister, & Bies, 1998; see also Adams & Sartori, 2005). *Distrust* is a separate, but related construct, which can be characterised as involving levels of fear, scepticism, cynicism, monitoring and vigilance. In addition, distrust involves a perception of malevolent intentionality. Events may arouse distrust or simply reduce trust. The former will be affected by the type of violation, its centrality and the attribution it invokes. Distrust can be affected by factors such as the distruster's propensity to distrust, his/her goals, and judgment biases/errors (e.g., attribution error); perceptions of the distrustee's values, attitudes and intentions, as well as reputation and group membership; group or organisational context, structure and norms. Both trust and distrust are affected by the level of risk, vulnerability and uncertainty in an environment or situation. Both constructs lead to varying levels of conflict, monitoring, cooperation, enacting of control strategies, and interpersonal distress (although these consequences are more intense under distrust and obviously differ in directionality). In addition, distrust may lead to biased information processing, self-focus, hyper-vigilance, and rumination, as well as motivation for revenge.

3.10 *Psychological profiling* can help to identify an individual's personal characteristics (e.g., cognitive processes, behaviours and habits) useful for shaping and predicting his/her behaviour (Mann, 2008). For instance, DI HF produces profiles (called psychological assessments) of targets, and the police use criminal profiling. Constructing a profile involves collecting and analysing data about the individual. Data may be collected from open sources and/or intelligence. Analysis may be

'clinical' (i.e., based on the profiler's intuition, experience and knowledge) or 'statistical' (i.e., based on comparison with characteristics of others who fit the data pattern). However, there is little evidence to suggest that profiling leads to accurate predictions (Snook, Eastwood, Gendreau, Goggin, & Cullen, 2007). In addition, although knowledge of an individual's personality may increase our ability to predict his/her behaviour, behaviour may be affected by time and situation, and so an interactionist approach may prove more useful (Mischel, 1973).

3.11 Social psychological knowledge has been applied to *advertising* and *marketing* (Clow & Baack, 2007; Kahle & Kim, 2006). Marketing approaches help to identify the target audience, as well as predict and meet their needs. Different types of advertising can increase people's awareness and knowledge of an item/issue, their liking, preference and support for it, and encourage behavioural acquisition of it. Knowledge of concepts such as branding, product placement, sales promotions, niche marketing, crowd sourcing, herd behaviour, market segmentation, public relations, and viral advertising/marketing may be particularly relevant for JTRIG's effects and online HUMINT operations. In addition internet/digital/online/web or e-marketing and advertising can indicate how these concepts and approaches are applied in cyberspace.

3.12 Of particular relevance to the cyber-based effects and online HUMINT operations conducted by JTRIG is that researches have begun to study *behaviour in cyberspace*, including social influence. For instance, studies have found that anonymous groups may be more susceptible to influence than identifiable groups (Postmes, Spears, Sakhel, & de Groot, 2001). People in online social networks make new links with those whom they perceive to be similar (Crandall et al., 2008), and they are more likely to view a YouTube video if they believe others similar to them have viewed and liked it (Marcus & Perez, 2007). Neighbours/friends in online social networks are also more powerful than strangers in persuading a user to join an online group (Hui & Buchegger, 2009). The ability to trigger replies from others, create conversations between others, and induce similarity of language among users is more likely to be found in "online leaders" who demonstrate high communication activity, longer group membership, expansive and reciprocal social networks, and language use characterised by talkativeness, diversity, assertiveness, and emotion (Huffaker, 2010). High numbers of chat room contributions and words, as well as high levels of assertiveness and exaggeration can have a significant influencing effect during anonymous computer-mediated discourse (Miller & Brunner, 2008). Finally, during computer-mediated interaction, females are more likely to conform when the other party expresses confidence in their expertise verbally, whereas males are more likely to be influenced by quantitative expressions of confidence (Lee, 2005). Male online characters are also more likely to induce informational influence than female ones.

3.13 One important caveat to the psychological work on the above topics is that it has for the most part been based on limited samples of the human population (e.g., White, middle-class, American, male, students). This lack of representativeness means that the theories and research findings may not be generalisable to other populations (e.g., other ethnicities, less educated, females, older adults, other cultures). For instance, attribution processes differ in collectivist and individualistic

cultures in that collectivist (mainly non-Western) cultures are more likely to attribute a person's behaviour to situational rather than dispositional/personality causes, and so dissonance is less in collectivist cultures (e.g., Nagayama Hall & Barongan, 2002). Collectivist cultures also demonstrate a greater tendency for conformity, and levels of obedience vary across social contexts (Smith & Bond, 1998). Therefore, when planning effects and online HUMINT operations, JTRIG staff should avoid ethnocentrism, and understand the psycho-social processes common to the culture they wish to engage with.

Psycho-Criminological Approaches to Influencing Prevention

3.14 The overall goal of JTRIG's effects and online HUMINT operations is to combat external threats at source. These threats may be actual or potential, and they may be eliminated or reduced. The specific objectives of the operations are not unlike some of those strived for by the formal criminal justice system such as prevention, deterrence and incapacitation. For example, posing as a vendor trading in uranium and taking payment from an individual or group who wishes to purchase products necessary for building a nuclear weapon would financially incapacitate them from purchasing such products from an actual vendor. Beyond the delay effects due to incapacitation, it may also deter them or others from engaging in this type of business transaction in the future. However, incapacitation is typically temporary, and there is little evidence for the deterrence effects of incapacitation (e.g., von Hirsch, Bottoms, Burney, Wikstrom & 1999; Gendreau & Goggin, 1999). Alternatively, prevention may be a more effective means of dealing with threats. Thus, JTRIG's operations may benefit from being informed by the theoretical and empirical work on crime prevention.

3.15 Of particular relevance to the targets that JTRIG typically focuses on, a situational crime prevention approach has been proposed for dealing with terrorism (see Freilich & Newman, 2009). This includes terrorist hostage taking in Afghanistan (Yun, 2009) and far-right activists (Freilich & Chermak, 2009). It is also suggested that intelligence work should focus on gathering information relevant for prevention of terrorism (Newman, 2009). The roots of situational crime prevention approaches in conceptions of the offender's decision making are briefly described below.

3.16 Rational choice theories of offender behaviour posit that individuals attach values to the possible rewards and costs associated with an action, calculate the probabilities of these rewards and costs, weight the values of reward and costs by their respective probabilities, and choose the course of action that maximises gains and minimizes losses (see Becker, 1968). There is some (mostly qualitative) evidence to support this approach (e.g., Carroll & Weaver, 1986), and it has practical implications for crime prevention. In fact, the Home Office's situational crime prevention agenda is rooted in the rational choice approach. It is suggested that "crime can be prevented by reducing opportunities" (Felson & Clarke, 1998, p. vi). Prevention techniques may focus on: (1) increasing the perceived effort involved in committing crime; (2) increasing the perceived risks; (3) reducing the anticipated rewards; and (4) removing excuses for crime. The perceived effort can be increased

by, for example, target hardening, controlling access to targets, and deflecting offenders from targets (see Clarke, 1997). The perceived risk of crime can be increased by surveillance. The anticipated rewards of crime can be reduced by, for example, removing targets, reducing temptation, and denying benefits. Finally, excuses for crime can be reduced by, for example, alerting conscience, controlling disinhibitors, and assisting compliance. (Note, that in this literature "target" refers to person or property that may be victimized, which is not to be confused with JTRIG's use of the term to represent the individuals or groups who are the subject of operations).

3.17 By contrast to the above rational choice approach, there are also views of offenders' rationality that emphasize its bounded or limited nature (e.g., Johnson & Payne, 1986; Tunnell, 2002). Rationality may be limited by, for example, limited time, information, resources, and cognitive processing capacity, as well as psychopharmacological agents. Recent evidence suggests that (actual and potential) offenders' intentions to engage in criminal activity are best predicted by their perceptions of the importance they attach to the benefits, regardless of their probabilities or the drawbacks and their probabilities (Dhami & Mandel, in press). In fact, individuals may be well aware of the potential drawbacks involved in a risky behaviour, but they also see potential benefits (Dhami, Mandel, & Garcia-Retamero, 2010). Other evidence also indicates that offenders' decisions to commit crimes are better predicted by simple heuristic processing where the vast majority of pertinent information is ignored, than by more complex processing that weights and integrates the available, relevant information (Garcia-Retamero & Dhami, 2009; Snook, Dhami, & Kavanagh, 2010). The practical implications of this bounded rationality approach are clear: Prevention efforts ought to identify and alter people's perceptions of the benefits of engaging in a risky (criminal) behaviour. Where possible, efforts could also be made to highlight acceptable alternatives to these behaviours that yield the desired benefits. Finally, prevention efforts could further emphasise the low probabilities of obtaining the benefits, the undesirability of the drawbacks, and the higher probabilities of incurring them.

3.18 More recently, a distinction has been made between "hard" and "soft" situational crime prevention techniques (Wortley, 2001, 2008). Unlike the former that manipulate situational factors, the latter manipulate psycho-emotional factors. Ideologically motivated crimes and those committed by non-violent, "mundane" offenders may be particularly suitable for soft measures. In fact, unlike hard techniques that may be easily detected, and so be provocative or countered, soft techniques are subtle, and also less susceptible to displacement. Some examples of soft techniques include: Reducing frustration and stress; avoiding disputes; posting instructions; neutralizing peer pressure; discouraging imitation; alerting conscience; and assisting compliance.

3.19 One important point to stress when combating threats and using crime prevention techniques is to understand their nature in detail and to identify the factors that may motivate and deter relevant individuals or groups. This can help to best tailor the technique to the individual target(s), and increase operational success.

3.20 Displacement represents one of the main risks of crime prevention techniques. Displacement may be geographical, temporal, target, tactical, or offence type. However, displacement is rarely 100%, and can sometimes be controlled (see Clarke, 1997). In fact, there may sometimes be a diffusion of benefits to other locations and victims.

4. Non-Technical Operational Planning and Management

4.1 In order for JTRIG to plan and conduct successful effects and online HUMINT operations there is a need to ensure best practice in terms of, for example, risk assessment, measurement of operational success, and staff conduct. This chapter provides guidance on how such best practice can be achieved.

Risk Assessment

4.2 JTRIG staff identified several potential risks associated with conducting effects and online HUMINT operations (see Chapter 2, para. 2.8 and 2.13). Assessing the potential risks involved in conducting an operation and how they can be avoided or mitigated is essential not only to the planning of an operation, but also to informing decisions about whether it should proceed and measuring its success. Below is a discussion of some of the main issues that ought to be considered in developing a comprehensive risk assessment process.

4.3 Risk assessments (including within JTRIG) commonly focus solely on the value of the costs and/or their probability of occurrence. This is only a partial assessment as it excludes the potential benefits and their probabilities. Thus, following Knight's (1921) comprehensive definition of risk, in order to compute the (subjective) expected utility of conducting an operation (see Savage, 1954), it is advisable to identify and calculate the magnitude of the benefits and multiply these by their probabilities, and then subtract the magnitude of the costs multiplied by their probabilities. The magnitude of the costs and benefits may be quantitatively and/or qualitatively defined (e.g., financial cost of operation and amount of extremist material taken off a website are quantitative costs and benefits, respectively; whereas being discovered and influencing distrust in a trader are qualitative costs and benefits). Similarly, probabilities may be defined in numerical or linguistic terms (e.g., 30% chance; very likely). Measures of variables may be objective and/or subjective. Both objective and subjective measures are susceptible to measurement error, however. Where objective measurements of the costs and benefits associated with an operation are difficult to come by, as is likely to be the case for JTRIG's operations, subjective ones may be acceptable. Here, estimates can be obtained from subject matter experts if they are available (SMEs; see e.g., Slottje, Sluijs, & Knol, 2008).

4.4 Some scholars have argued that in addition to computing the potential risk involved in engaging in a specific action, the potential risk involved in inaction should also be computed (Furby & Beyth-Marom, 1992). This more time and resource intensive approach has not been particularly popular, but it does allow for a more comprehensive assessment, and one that estimates the potential outcome in the absence of an operation.

4.5 A risk assessment should also involve identification of ways in which any unacceptable risks can be avoided or mitigated, and consideration of how successful such interventions might be.

4.6 Finally, the way in which the output of a risk assessment is interpreted is also important. For instance, there needs to be consistency in interpretation of the probabilities, particularly if they are expressed linguistically. Although interpretations of linguistic probabilities that may be used to communicate the probabilities associated with the costs and benefits of an operation are subject to both intra- and inter-individual unreliability, these can be reduced by a simple translation method (see Dhami & Wallsten, 2005). In addition, in the public health domain, the use of specific interventions is not allowed unless it can be demonstrated that they do not increase the risk to the sample or population of interest beyond an acceptable and agreed threshold (Fischoff, Lichtenstein, Slovic, Derby, & Keeney, 1981). It might be useful to develop a set of relevant thresholds for JTRIG's operations that set out the acceptable risk. This can be done using revealed- and expressed-preference methods (see e.g., McDaniels, 1988; Slovic, 1995).

Measurement of Operational Success

4.7 JTRIG staff identified several potential measures of operational success (see Chapter 2, para. 2.11). Measuring the effectiveness or success of an effects or online HUMINT operation is essential not only because it provides useful feedback to those who tasked and conducted the operation, but also because this information can be used to inform the development and implementation of future operations. Success measures also require clear specification of the goals and objectives of an operation. Below is a discussion of some of the main issues that ought to be considered in developing a comprehensive catalogue of operational success (or failure) measures.

4.8 Measures of operational success should be directly or indirectly related to the specific aims of the operation (e.g., to "discredit", promote "distrust," "dissuade", "deceive", "disrupt", "delay", "deny", "denigrate/degrade", and "deter").

4.9 When conducting operations whose main goal is to influence by changing attitudes, encouraging compliance, obedience or conformity, and persuade measures need to be taken in order to ascertain the following:

- Has the target attended to the message?
- Has the target understood the message?
- Has the target accepted the message?
- Has the target remembered the message?
- Has the target behaved in accordance with the message?

4.10 When conducting online HUMINT operations, measures need to be taken in order to ascertain the following:

- Stage of relationship with the target
- Closeness of relationship with the target

- Level of trust and distrust the target has in the alias
- Reliability and validity of intelligence provided by the target
- Amount of valid and reliable intelligence provided by the target
- Has the target provided sufficient information to conduct a psychological profile?

4.11 Measures of operational success also ought to consider the potential risks and benefits that have been identified in the risk assessment. Particular attention should be paid to the duration of the outcomes, displacement (i.e., geographical, temporal, target, tactical, or offence type), and diffusion of benefits to other locations and victims.

4.12 A distinction should also be made between direct and indirect measures of operational success, as well as objective and subjective measures. Greater weight should be given to direct and objective measures. Effort should also be made to have a combination of both quantitative and (intangible) qualitative measures, where appropriate.

Conduct Guidelines

4.13 Practitioners of all sorts, including the police and behavioural scientists, working with people, typically have to abide by a set of practice guidelines or codes of conduct that not only enshrine best practice, but also potentially guard practitioners from complaints and liability. Here, is a review of some of the main components of existing codes and guidelines that may be pertinent to JTRIG's operations.

4.14 Police powers and how those powers can be exercised are contained in the Police and Criminal Evidence Act 1984 (PACE; Home Office, 2011). Codes A and B of PACE deal with powers to stop, search and seize. Code C sets out the requirements for detention, treatment and questioning, and Code G sets out powers of arrest (Code H refers to terror suspects). Code D deals with the methods of identification and record keeping, while Codes E and F deal with recording interview data. The Serious Organised Crime and Police Act 2005 (SOCA; Home Office, 2005) similarly lays out, among other things, the powers of SOCA staff (including search and investigation); use and disclosure of information; treatment of offenders assisting in investigations and prosecutions; protection of witnesses and other persons (including activities of certain organisations); proceeds of crime; international obligations; and organisational liability for unlawful conduct. (See also the Criminal Procedure and Investigations Act 1996 code of conduct; Home Office, 1996).

4.15 According to the British Society of Criminology's (2011) code of ethics, researchers should ensure that the physical, social and psychological wellbeing of participants is not adversely affected by participation; seek participants' informed consent; protect the identity of participants and secure their data; and maintain good relations with funding bodies. Similarly, the British Psychological Society (2004,

2007, 2009) lays out the ethical principles of respect, competence, responsibility, and integrity. These embody standards of practice relating to, for example, privacy and confidentiality; informed consent; conflicts of interest; maintaining personal boundaries; safeguards for vulnerable populations; and appropriate supervision. Ethical issues pertaining to internet research have also been outlined and include for example, verifying identity, monitoring the consequences of research, and understanding public versus private space. Typically, ethical approval must be sought before research is conducted.

4.16 Clearly, not all of the aspects of the above codes will be relevant or applicable to JTRIG's operations. In addition, these codes do not identify best practice in all of the types of online interactions that JTRIG staff might be involved in. Thus, JTRIG may need to develop a bespoke code that in addition to other considerations complies with legislation such as the Regulation of Investigatory Powers Act 2000 (Home Office, 2000) that regulates how public bodies conduct surveillance and investigations, as well as intercept communications, and the Interception of Communications Act 1985 (Home Office, 1985). Staff will need to recognise the importance of compliance with any such code, and be aware of the potential organisational responses to non-compliance.

5. Conclusions and Recommendations

5.1 The importance of influence in cyberspace was highlighted in the recent National Security Strategy (NSS) and the Strategic Defence and Security Review (SDSR; UK Government, 2010a, 2010b). The SDSR states that "Strategic communications are important for our national security because they can positively change behaviours and attitudes to the benefit of the UK, and counteract the influence of dangerous individuals, groups and states. The NSS recognises that threats to the UK may involve the internet. Thus, one of the two objectives of the NSS is to apply "…all our instruments of power and influence to shape the global environment and tackle potential risks at source." (p. 22). In addition, the SDSR notes the FCO's goal to "influence more audiences." (p. 67).

5.2 JTRIG provides most of GCHQ's cyber effects and online HUMINT capability. Together, the Rest of the World, CT, and SMO groups target a range of individual, group and state actors across the globe who pose criminal, security and defence threats. JTRIG staff use a range of techniques to, for example, discredit, disrupt, delay, deny, degrade, and deter. The techniques include: uploading YouTube videos containing persuasive messages; establishing online aliases with Facebook and Twitter accounts, blogs and forum memberships for conducting HUMINT or encouraging discussion on specific issues; sending spoof emails and text messages as well as providing spoof online resources; and setting up spoof trade sites. JTRIG thus currently lies at the leading edge of cyber influence practice and expertise.

5.3 Based on interviewees with a sample of 22 JTRIG staff and seven other staff from GCHQ who support JTRIG's operations, the present report concludes that JTRIG's effects and online HUMINT capability can be further enhanced by behavioural science support and improvement of some of JTRIG's non-technical operational planning and management. This chapter provides recommendations on how to implement such support and improvement.

Recommendations for Behavioural Science Support

5.4 As Chapter 3 outlines, JTRIG's effects and online HUMINT operations can be grounded in scientific theory and evidence from social psychology (i.e., social cognition, attitudes, persuasive communications, conformity, obedience, interpersonal relationships, trust and distrust, and psychological profiling), including its applications to advertising and marketing, and from criminology (i.e., crime prevention).

5.5 To some extent, some JTRIG staff already employ some of the techniques mentioned, and so these could be labelled as such. For instance, impression management/self-presentation can be used to influence by mimicking or imitating others' behaviour. This technique is evident in the mimicking of popular or relevant YouTube videos, Facebook profiles, censored news sites, and language used in

online business transactions. Reciprocity can be used to achieve compliance. This technique is demonstrated by providing useful information to extremists, hackers, and online criminals. However, there remains ample opportunity to expand JTRIG's techniques.

5.6 *Recommendation 1*. Chapter 3 describes behavioural techniques that can be used to influence. It is recommended that JTRIG trains its' staff to understand and appropriately apply such techniques, which are listed in Annex A (see also Chapter 3). Annex B provides a list of reading material that may be useful for training.

5.7 *Recommendation 2*. Chapter 3 cautions that the past social psychological research on influence has typically been limited to western cultures (and individuals) and face-to-face interactions. It is recommended that Dstl develops a research programme that: (1) measures the generalisability of specific social influence techniques across cultural groups representative of the types of targets of interest to defence and security organisations such as non-western cultures, business and consumer cultures, and opportunistic/individual versus professional/organised offenders, so that techniques can be applied appropriately. And (2) reviews the body of work on influence in cyberspace in order to inform cyber influence operations.

5.8 *Recommendation 3*. Chapter 3 notes the widespread use of personality profiling in the criminal justice system. It is recommended that Dstl develops a programme of work that assesses the feasibility of compiling personality profiles based on information available about the individual on the internet (and perhaps through covert surveillance and/or developing online relations for HUMINT purposes), so that those conducting online HUMINT can compile and exploit such profiles.

5.9 *Recommendation 4*. Chapter 3 also discusses the popularity of crime prevention techniques. It is recommended that Dstl (1) reviews the extant literature identifying the cost-benefit factors that motivate individuals to commit specific types of criminal activity (especially online). And, (2) develops a catalogue of soft crime prevention techniques and those that focus on perceived importance/value of benefits to the target that can be applied online.

Recommendations for Improving Operational Planning and Management

5.10 As Chapter 4 outlines, the effectiveness of JTRIG's effects and online HUMINT operations can be enhanced by improving the current process of assessing the risks associated with conducting operations and the measurement of operational success, and by providing staff with practice/conduct guidelines.

5.11 *Recommendation 5*. Chapter 2 identifies operational risks and Chapter 4 describes a *comprehensive* approach to risk assessment. It is recommended that JTRIG designs an operational risk assessment process focusing on the magnitude and probability of both the costs and benefits of conducting and (perhaps not conducting) an operation. Objective and/or subjective, quantitative and/or qualitative

measures of the outcomes should be identified so they can be applied consistently. Potential general risk mitigation strategies and acceptable risk thresholds should also be identified where possible. Finally, efforts should be made to provide a scale that can be used to consistently interpret the output of risk assessments.

5.12 *Recommendation 6*. Several measures of operational success are listed in Chapters 2 and 4. It is recommended that JTRIG develops a catalogue of quantitative and qualitative, direct and indirect measures that provide reliable and valid data on the effectiveness of online effects and HUMINT operations.

5.13 *Recommendation 7*. Chapter 4 discusses the applicability of practice guidelines/conduct codes for JTRIG's staff. It is recommended that JTRIG develops relevant guidelines or a code describing best practice when conducting operations.

5.14 Annex C presents a list of training requirements for JTRIG staff that incorporates the issues discussed in the present report (including recommendations 1 and 5 to 7). In addition to this, JTRIG may want to consider whether staff recruitment could target social scientists. The advantages and limitations of having staff specialising in specific techniques versus being generalists may also need to be considered.

Final Remarks

5.15 Recommendations 1 and 5 to 7 refer to delivery of support and improvement in the short-term that can have immediate and durable benefits for JTRIG's operational work. For the most part, these recommendations can be implemented by JTRIG itself, with some assistance from OMG's and legal advisors, and possibly those experienced in teaching professional groups applied psychology/criminology. Although the Defence Academy at Shrivenham has a course on information operations, it is unclear if it covers influence in cyberspace, targets relevant to JTRIG's operations, and influence to achieve the typical aims of JTRIG's operations. Given that JTRIG has an in-house training capability, a bespoke training module might not only be more effective, but also more convenient for staff and easy to monitor/revise as JTRIG develops.

5.16 Recommendations 2 to 4 refer to delivery of support in the medium- to long-term that can have durable benefits for those conducting cyber influence operations. The implementation of these recommendations can be managed by Dstl. In doing so, Dstl may wish to refer to relevant expertise across Defence and Government such as the Behavioural Sciences Unit (BSU), as well as industry and academia. The BSU has established links with JTRIG. Although there has been a debate recently as to whether academics should be involved in military social influence campaigns (see King, 2011), Dhami (2011) highlights the unique expertise that such psychological scholars have in terms of interpreting the practical applicability of existing theories of social influence as well as making theoretical advances useful for developing practically relevant non-social influence techniques.

5.17 Targets can and will adapt to changes, and it is wise to think ahead and laterally in order to anticipate adaptation levels in order to combat these. In order for JTRIG to remain at the leading edge of cyber-based effects and online HUMINT operations, it will need to consider the potential practical utility of emerging social and non-social psychological and criminological theories for effecting influence against threats in cyberspace.

References

Adams, B. D., & Sartori, J. A. (2005). *The dimensionality of trust*. DRDC Toronto No. CR-2005-204.

Bachmann, R., & Zaheer, A. (2006). (Eds.), *Handbook of trust research.* Cheltenham: Edward Elgar Publishing.

Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy,76*, 169-217.

British Psychological Society (2009). *Code of ethics and conduct*. Retrieved from http://www.bps.org.uk/document-download-area/document-download$.cfm?file_uuid=E6917759-9799-434A-F313-9C35698E1864&ext=pdf

British Psychological Society (2007). *Conducting research on the internet: Guidelines for ethical practice in psychological research online*. Retrieved from http://www.bps.org.uk/document-download-area/document-download$.cfm?file_uuid=2B3429B3-1143-DFD0-7E5A-4BE3FDD763CC&ext=pdf

British Psychological Society (2004). *Guidelines for minimum standards of ethical approval in psychological research*. Leicester: British Psychological Society.

British Society of Criminology (2011). *Code of ethics*. Retrieved from http://www.britsoccrim.org/codeofethics.htm

Carroll, J., & Weaver, F. (1986). Shoplifters' perceptions of crime opportunities: A process-tracing study. In D. B. Cornish, & R. V. Clarke (Eds.), *The reasoning criminal* (pp. 19-38). New York: Springer-Verlag.

Cialdini, R. B. (2009). *Influence: Science and practice*. Boston: Allyn & Bacon.

Clarke, R. V. (1997). *Situational crime prevention: Successful case studies*. Second Edition. Albany, NY: Harrow & Heston.

Clow, K. E., & Baack, D. (2007). *Integrated advertising, promotion, and marketing communications.* Upper Saddle River, NJ: Pearson Education.

Crandall, D., Cosley, D., Huttenlocher, D., Kleinberg, J., & Suri, S. (2008). Feedback effects between similarity and social influence in online communities. *KDD*.

Dhami, M. K. (2011). Military social influence: Commentary on King. *Analyses of Social Issues and Public Policy*, *11*.

Dhami, M. K., & Mandel, D. R. (in press). Crime as risk taking. *Psychology, Crime and Law.*

Dhami, M. K., Mandel, D. R., & Garcia-Retamero, R. (2010). Canadian and Spanish youths' risk perceptions of drinking and driving, and riding with a drunk driver. *International Journal of Psychology.*

Dhami, M. K., & Wallsten, T. S. (2005). Interpersonal comparison of subjective probabilities. *Memory & Cognition, 33*, 1057-1068.

Felson, M., & Clarke, R. V., (1998). *Opportunity makes the thief. Practical theory for crime prevention*. Police Research Series Paper 98. London: Home Office.

Fischoff, B., Lichtenstein, S., Slovic, P., Derby, S. K., & Keeney, R. (1981). *Acceptable risk*. Cambridge, UK: Cambridge University Press.

Fiske, S. T. (2010). *Social beings: Core motives in psychology*. Hoboken, NJ: John Wiley & Sons.

Fiske, S. T., Gilbert, D. T., & Lindzey, G. (2010). (Eds.), *Handbook of social psychology*. New York: Wiley.

Forgas, J. P., Cooper, J., & Crano, W. D. (2010). (Eds.), *The psychology of attitudes and attitude change.* London: Psychology Press.

Freilich, J. D., & Chermak, S. M. (2009). Preventing deadly encounters between law enforcement and American far-rightists. *Crime Prevention Studies, 25*, 141-172.

Freilich, J. D., & Newman, G. R. (2009). (Eds.), Reducing terrorism through situational crime prevention. *Crime Prevention Studies, 25*. Cullompton: Willan Publishing.

Furby, L., & Beyth-Marom, R. (1992). Risk taking in adolescence: A decision-making perspective. *Developmental Review, 12*, 1-44.

Garcia-Retamero, R., & Dhami, M. K. (2009). Take-the-best in expert-novice decision strategies for residential burglary. *Psychonomic Bulletin & Review, 16* 163-169.

Gendreau, P., & Goggin, C. (1999). The effects of prison sentences on recidivism. Retrieved from http://www.prisonpolicy.org/scans/e199912.htm

Hogg, M. A., & Vaughan, G. M. (2008). *Social psychology: An introduction*. Essex: Pearson.

Home Office (1996). Criminal Procedure and Investigations Act 1996. Retrieved from http://www.legislation.gov.uk/ukpga/1996/25/contents

Home Office (1985). Interception of Communications Act 1985. Retrieved from http://www.legislation.gov.uk/ukpga/1985/56/contents

Home Office (2011). *Police and Criminal Evidence Act 1984 (PACE) and accompanying codes of practice*. Retrieved from http://www.homeoffice.gov.uk/publications/police/operational-policing/pace-codes/

Home Office (2000). Regulation of Investigatory Powers Act 2000. Retrieved from http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice

Home Office (2005). *Serious Organised Crime and Police Act 2005*. Retrieved from http://www.legislation.gov.uk.ukpga/2005/15/contents

Horowitz, L. M., & Strack, S. (2011). *Handbook of interpersonal psychology: Theory, research, assessment and therapeutic interventions.* Hoboken, NJ: John Wiley & Sons.

Huffaker, D. (2010). Dimensions of leadership and social influence in online communities. *Human Communication Research, 36*, 593-617.

Hui, P., & Buchegger, S. (2009). Groupthink and peer pressure: Social influence in online social network groups. *Asonam. International Conference on Advances in Social Network Analysis and Mining,* 53-59.

Johnson, E., & Payne, J. (1976). The decision to commit a crime: An information processing analysis. In D. B. Cornish, & R. V. Clarke (Eds.), *The reasoning criminal* (pp. 170-185). New York: Springer-Verlag.

Kahle, L. R., & Kim, C. (2006). (Eds.). *Creating images and the psychology of marketing communication*. Mahwah, NJ: Lawrence Erlbaum Associates.

King, S. B. (2011). Military social influence in the global information environment: A civilian primer. *Analyses of Social Issues and Public Policy, 11*.

Knight, F. H. (1921/1964). *Risk, uncertainty, and profit*. New York: Sentry Press.

Lee, E. (2005). Effects of the influence agent's sex and self-confidence on informational social influence in computer-mediated communication. *Communication Research, 32*, 29-58.

Lewicki, R., McAllister, D., & Bies, R. (1998). Trust and distrust: New relationships and realities. *Academy of Management Review, 23*, 438-455.

Maio, G. R., & Haddock, G. (2009). *The psychology of attitudes and attitude change*. London: Sage.

Mann, I. (2008). *Hacking the human: Social engineering techniques and security and countermeasures*. Hampshire: Gower Publishing Limited.

Marcus, A., & Perez, A. (2005). m-YouTube Mobile UI: Video selection based on social influence. *Human-Computer Interaction,* 926-932.

McDaniels, T. L. (1988). Comparing expressed and revealed preferences for risk reduction: Different hazards and question frames. *Risk Analysis, 8*, 593-604.

Miller, M. D., & Brunner, C. C. (2008). Social impact in technologically-mediated communication: An examination of online influence. *Computers in Human Behavior, 24*, 2972-2991.

Mischel, W. (1973). Toward a cognitive social learning reconceptualisation of personality. *Psychological Review, 80*, 252-283.

Nagayama Hall, G. C., & Barongan, C. (2002). *Multicultural psychology*. Upper Saddle River, NJ: Prentice-hall.

Newman, G. R. (2009). Reducing terrorist opportunities: A framework for foreign policy. *Crime Prevention Studies, 25*, 33-59.

Pettigrew, T. F., & Tropp, L. R. (2006). A meta-analytic test of intergroup conflict theory. *Journal of Personality & Social Psychology, 90*, 751-783.

Postmes, T., Spears, R., Sakhel, K., & de Groot, K. (2001). Social influence in computer-mediated communication: The effects of anonymity on group behaviour. *Personality and Social Psychology Bulletin, 27*, 1242-1254.

Savage, L. J. (1954). *The foundations of statistics*. New York: Wiley.

Slottje, P., Sluijs, J. P. van der, & Knol, A. B. (2008). Expert elicitation: Methodological suggestions for its use in environmental health impact assessments. Retrieved from http://www.nusap.net/downloads/reports/Expert_Elicitation.pdf

Slovic, P. (1995). The construction of preference. *American Psychologist, 50*, 364-371.

Smith, P. B., & Bond, M. H. (1998). *Social psychology across cultures* (2nd Edition). Hemel Hempstead: Prentice-Hall.

Snook, B., Dhami, M. K., & Kavanagh, J. (2010). Simply criminal: Predicting burglars' occupancy decisions with a simple heuristic. *Law and Human Behavior.*

Snook, B., Eastwood, J., Gendreau, P., Goggin, C., & Cullen, R. M. (2007). Taking stock of criminal profiling: A narrative review and meta-analysis. *Criminal Justice and Behavior, 34*, 437-453.

Tunnell, K. D. (2002). The impulsiveness and routinization of decision-making. In A. R. Piquero, & S. G. Tibbets (Eds.), *Rational choice and criminal behaviour: Recent research and future challenges* (pp. 265-278). New York: Routledge.

UK Government (2010a). A strong Britain in an age of uncertainty: National Security Strategy. London: The Stationary Office.

UK Government (2010b). A strong Britain in an age of uncertainty: Strategic Defence and Security Review. London: The Stationary Office.

von Hirsch, A., Bottoms, A., Burney, E., & Wikstrom, P-O. (1999). *Criminal deterrence and sentencing severity*. Oxford: Hart Publishing.

Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. *Security Journal, 14*, 63-82.

Wortley, R. (2008). Situational precipitators of crime. In R. Wortley, & L. Mazerolle (Eds.), *Environmental criminology and crime analysis.* Cullumpton: Willan.

Yun, M. (2009). An application of situational crime prevention to terrorist hostage taking and kidnapping: A case study of 23 Korean hostages in Afghanistan. *Crime Prevention Studies, 25*, 111-139.

Annex A

Examples of Social Influence Techniques and Other Relevant Behavioural Approaches

Impression Management/Self-presentation:

- Matching others' behaviour
- Conforming to situational norms
- Ingratiation
- Consistency of self
- Self-promotion
- Credible intimidation
- Exemplary behaviour and
- Supplication (i.e., needing help)

Persuasive Communication:

- Recipient must have access to the message
- Recipient must attend to the message
- Recipient must understand the message
- Recipient must accept the message
- Recipient must remember the message
- Recipient must behave according to the message

Propaganda:

- Using stereotypes
- Substituting names/labels for neutral ones
- Censorship or systematic selection of information
- Repetition
- Assertions without arguments
- Presenting a message for and against a subject

Reducing Prejudicial Attitudes:

- Increasing contact with the person or object against which the prejudice is directed. This contact should be:
    - Of equal status
    - In a cooperative context
    - Frequent
    - Not anxiety or threat inducing
    - Encouraging positive cross-group relations

Encouraging Obedience:

- Engaging the norm of reciprocity
- Engendering liking (e.g., via ingratiation or attractiveness)
- Stressing the importance of social validation (e.g., via highlighting that others have also complied)
- Instilling a sense of scarcity or secrecy

- Getting the “foot-in-the-door” (i.e., getting compliance to a small request/issue first)
- Applying the “door-in-the-face” or “low-ball” tactics (i.e., asking for compliance on a large request/issue first and having hidden aspects to a request/issue that someone has already complied with, respectively)

Discouraging Obedience:

- Educating people about the adverse consequences of compliance
- Encouraging them to question authority
- Exposing them to examples of disobedience

Encouraging Majorities to Conform to Minorities:

- Showing a sense of consistency
- Demonstrated investment
- Independence
- Balanced judgment
- Similarity to the majority in terms of age, gender and social category.

Beginning and Maintaining Interpersonal Relationships:

- Proximity
- Exposure
- Familiarity
- Similarity
- Physical attractiveness
- Reciprocal self-disclosure

Encouraging Distrust:

- Perceptions of the distrustree’s values, attitudes and intentions
- Perceptions of the distrustree’s reputation
- Perceptions of the distrustree’s group membership
- Group or organisational context, structure and norms

Crime Prevention:

- Identify and alter perceptions of the benefits
- Highlight acceptable alternatives that yield the desired benefits
- Emphasise the low probabilities of obtaining the benefits
- Emphasise the undesirability of the drawbacks
- Emphasise the higher probabilities of incurring the drawbacks
- Soft techniques:
    - Reducing frustration and stress
    - Avoiding disputes
    - Posting instructions
    - Neutralizing peer pressure
    - Discouraging imitation
    - Alerting conscience
    - Assisting compliance

Relevant Issues in Advertising and Marketing:

- Branding
- Product placement
- Sales promotions
- Niche marketing
- Crowd sourcing
- Herd behaviour
- Market segmentation
- Public relations
- Viral advertising/marketing
- Internet/digital/online/web or e- marketing and advertising

Annex B

Recommended Reading List for Relevant Behavioural Science Support

*JTRIG has now acquired this material.

Adams, B. D., & Sartori, J. A. (2005). *The dimensionality of trust*. DRDC Toronto No. CR-2005-204.

*Bachmann, R., & Zaheer, A. (2006). (Eds.), *Handbook of trust research.* Cheltenham: Edward Elgar Publishing.

*Cialdini, R. B. (2009). *Influence: Science and practice*. Boston: Allyn & Bacon.

Clow, K. E., & Baack, D. (2007). *Integrated advertising, promotion, and marketing communications.* Upper Saddle River, NJ: Pearson Education.

*Dhami, M. K., & Mandel, D. R. (in press). Crime as risk taking. *Psychology, Crime and Law.*

*Fiske, S. T. (2010). *Social beings: Core motives in psychology*. Hoboken, NJ: John Wiley & Sons.

Fiske, S. T., Gilbert, D. T., & Lindzey, G. (2010). (Eds.), *Handbook of social psychology*. New York: Wiley.

*Forgas, J. P., Cooper, J., & Crano, W. D. (2010). (Eds.), *The psychology of attitudes and attitude change.* London: Psychology Press.

*Garcia-Retamero, R., & Dhami, M. K. (2009). Take-the-best in expert-novice decision strategies for residential burglary. *Psychonomic Bulletin & Review, 16* 163-169.

Hogg, M. A., & Vaughan, G. M. (2008). *Social psychology: An introduction*. Essex: Pearson.

*Horowitz, L. M., & Strack, S. (2011). *Handbook of interpersonal psychology: Theory, research, assessment and therapeutic interventions.* Hoboken, NJ: John Wiley & Sons.

Kahle, L. R., & Kim, C. (2006). (Eds.). *Creating images and the psychology of marketing communication*. Mahwah, NJ: Lawrence Erlbaum Associates.

Lewicki, R., McAllister, D., & Bies, R. (1998). Trust and distrust: New relationships and realities. *Academy of Management Review, 23*, 438-455.

Maio, G. R., & Haddock, G. (2009). *The psychology of attitudes and attitude change*. London: Sage.

Mann, I. (2008). *Hacking the human: Social engineering techniques and security and countermeasures*. Hampshire: Gower Publishing Limited.

Nagayama Hall, G. C., & Barongan, C. (2002). *Multicultural psychology*. Upper Saddle River, NJ: Prentice-hall.

*Smith, P. B., & Bond, M. H. (1998). *Social psychology across cultures* (2nd Edition). Hemel Hempstead: Prentice-Hall.

Wortley, R. (2008). Situational precipitators of crime. In R. Wortley, & L. Mazerolle (Eds.), *Environmental criminology and crime analysis.* UK: Cullumpton.

Annex C

Suggested Components of Training Module for JTRIG

Training exercises ought to:

(1) Provide the scientific and technical, and operational planning and management knowledge (see list below) necessary for conducting successful, secure and safe effects and online HUMINT operations.
(2) Examine how well material has been understood.
(3) Apply knowledge to practical applications.
(4) Examine performance in practice.

Scientific and Technical Knowledge

(Social) scientific:

- Human behaviour in cyberspace
- Psychology of (social) influence
- Psychology applied to advertising and marketing
- Personality psychology and profiling
- Psychology of trust and distrust, and relationships
- Rational choice approaches to crime and crime prevention techniques
- Cultural psychology
- Scientific methods and analysis

Technical:

- Target capabilities
- Internet profiling
- Creating videos, photos, and other media
- Building websites and other web platforms
- ETC

Operational Planning and Management Knowledge

Planning operations:

- Specifying goals
- Selecting methods/techniques
- Predicting outcomes
- Assessing risk
- Identifying measures of effectiveness/success/outcomes
- Operational security
- Legal and policy mandates
- JTRIG's code of conduct/practice guidelines
- Deconfliction protocols
- Governance process

Managing operations:

- Continued risk assessment

- Measuring effectiveness/success/outcomes
- Report write-up
- Operational debrief

Fight "Gang Stalking"

Expose illegal stalking by corrupt law enforcement personnel

Tactics for Fighting Back

(https://fightgangstalking.files.wordpress.com/2013/05/little-red-riding-hood-by-lora-zombie-cropped.jpg)

Artist: Lora Zombie Click image to expand.

(https://fightgangstalking.files.wordpress.com/2013/05/blue-line3.jpg)

Contents

(https://fightgangstalking.files.wordpress.com/2013/05/blue-line3.jpg)

A. General Strategy

"What is of supreme importance in war is to attack the enemy's strategy."
– Sun Tzu, *The Art of War*

1. Shine a light on the cockroaches.

(https://fightgangstalking.files.wordpress.com/2013/05/spotlight.jpg)

Organized stalking is a manifestation of the view that intelligence and law enforcement agencies, their corporate cronies, and the military-industrial complex should have supremacy over all other elements of American government.

Even if you think that is a desirable power structure for national security reasons, it is impossible to deny that it grossly violates core principles of the U.S. Constitution. Organized stalking also violates stalking prohibitions under federal law and state laws in all fifty states.

One of the implications of that is that the perpetrators need to keep it a secret.

This is a primary difference between the use of organized stalking as a domestic counterintelligence strategy in America today and its use by the Stasi (state police) in communist East Germany: in the U.S. it is illegal.

This was true during the original version of COINTELPRO also – and was a primary reason the U.S. Senate conducted its Church Committee investigations after the FBI's activities were exposed by civilian activists.

Many of the tactics and strategies employed by the Stasi were virtually identical to those now used (and largely out-sourced apparently) by the FBI and other agencies in the U.S.

In East Germany however, the Stasi *wanted* citizens to be aware that their society was infested with spies because it furthered the communist party's goal of political control. In the U.S., such a public awareness would trigger a backlash against the abuse of power by the government and its cronies, so it is kept under the radar.

So the Achilles' heel of gang stalking is exposure.

From the perspective of intelligence and law enforcement agencies and corporations which use organized stalking as a secret illegal weapon for subversion, the perfect operation is one in which the target becomes progressively isolated, impoverished, emotionally degraded, and eventually commits suicide. That does happen in some cases – the most prominent example being the FBI's psychological torture of actress and political activist Jean Seberg. (https://fightgangstalking.com/#fbimemo)

Seberg's case was tactically successful in the short term (they destroyed her emotionally), but it was ultimately a strategic failure for the FBI because its crimes against her ended up on the front pages of national newspapers.

Without question, the vast majority of Americans do not want to live in a society infested with spies working for a Stasi-type government. To the extent that you can educate your fellow citizens about the creepy and illegal stalking activities of private security mercenaries, vigilantes, and corrupt law enforcement officers, they will be on your side.

Targets of organized stalking must wage a two-front war: we must act locally to expose the harassment to neighbors and others, and we must expose what is happening on a national level as well. Both objectives are critical.

---

2. Take calculated risks.

(https://fightgangstalking.files.wordpress.com/2013/05/f1-pass.jpg)

A strategic axiom in all arenas of competition and warfare is that the side which is at a disadvantage should be more aggressive. In a sports game, the team with a points lead can often exploit its position by playing cautiously. Conversely, the opponent with the points deficit has a logical incentive to take more risks.

Targeted individuals need to exploit asymmetrical warfare principles. As much as possible, we should employ tactics which are unpredictable, creative, cheap, simple and bold. The worst thing a victim of organized stalking could do would be to adopt a cautious, defensive posture.

Counterintelligence subversion is based on a strategy of intimidating the victim to the point that he or she is afraid to go anywhere or do anything without being constantly vigilant. That mental state cannot be sustained for a long period and it diverts energy and time and resources which could otherwise be devoted to exposing the criminals who orchestrate and perpetrate the stalking.

Organized stalking is cowardly and illegal, but it is not strategically stupid; it employs tactics which are effective, and difficult to prove legally. Also, it exploits the superior financial and political resources of the corrupt agencies and their corporate cronies which use it as a weapon.

We need to change the whole game and play it on our terms. Give the perps and their handlers some reasons to be uncomfortable. The way to throw a wrench into the Stasi machine is to expose its crimes to the public. Sometimes that requires stepping outside of your comfort zone a bit.

By the way, an additional benefit of adopting an offensive strategy is that when you are focused on working aggressively to undermine the criminals, the emotional effects of their harassment will diminish greatly.

Civil Disobedience

(https://fightgangstalking.files.wordpress.com/2013/05/mark-twain-on-patriotism.png)

Anyone who is already officially or unofficially blacklisted, should exploit that by taking the game to the gang stalkers. This is not to say that you have *nothing* to lose: you should avoid doing things which could lead to serious legal trouble. Fortunately, most of the tactics on this webpage are 100 percent legal, and the few which are in a grey area are acts of non-violent civil disobedience.

Incidentally, civil disobedience is a well-established, respected, and morally legitimate way to protest injustices. For targets of criminal harassment by corrupt members of law enforcement agencies and security contractors, it is even more than that; it is a necessary form of self-defense.

You do not need to wade more deeply into the philosophy of civil disobedience for the purposes of understanding its role in fighting gang stalking (or fighting corruption generally), but if you want to pursue the subject, you might want to start with this classic essay by Henry David Thoreau: *Civil Disobedience (https://fightgangstalking.files.wordpress.com/2013/05/civil-disobedience.pdf)*

Another essential document on the subject is "Letter from Birmingham Jail" (http://mlk-kpp01.stanford.edu/index.php/resources/article/annotated_letter_from_birmingham/) by Martin Luther King, Jr. In addition to being among America's most famous proponents of civil disobedience, King was a target of intense systematic persecution by lawless thugs in the FBI.

Several things are worth noting about the example of Martin Luther King, Jr. Although he was the target of cowardly and illegal harassment by creeps in a rogue law enforcement agency, he never bowed to their efforts at intimidation. Also note that King is now honored by a national holiday – whereas FBI Director J. Edgar Hoover is mostly reviled.

The Streisand Effect

One of the reasons that most of the tactics listed here do not involve much risk for the targeted individual is that gang stalking perps have to worry about the following phenomenon.

The "Streisand Effect" is when an effort to suppress information inadvertently causes an increase in attention to the information.

An online archive of 12,000 photographs of the California coastline – created to document coastal erosion – contained an aerial photograph (seen below) which included the Malibu mansion of singer and actress Barbra Streisand.

In 2003 Streisand filed a lawsuit to remove the photograph from the archive on the grounds that it violated her privacy. A judge eventually dismissed the lawsuit, but news coverage of the litigation brought much more attention to the photograph than it would otherwise have received.

Before Streisand filed her lawsuit, "Image 3850" had been downloaded from Adelman's website only six times; two of those downloads were by Streisand's attorneys. As a result of the case, public knowledge of the picture increased substantially; more than 420,000 people visited the site over the following month. – Wikipedia

Click on image to enlarge.

(https://fightgangstalking.files.wordpress.com/2013/05/streisand_estate-cropped.jpg)

Barbra Streisand's Mansion

Gang stalking perps (including corrupt members of local law enforcement agencies) will not want to attract attention to their gang stalking crimes by doing battle with you in a public way, so they have to be very reserved in their efforts to suppress your exposure of what is happening. You should exploit that.

Incidentally, I don't mean to bash Barbra Streisand – who, for example, offered her assistance to whistle-blower Daniel Ellsberg (http://www.democracynow.org/blog/2013/2/6/part_2_daniel_ellsberg_and_jacob_appelbaum_on_the_ndaa_wikileaks_and_unconstitutional_surveillance) when he was facing serious legal danger because of his revelation of the Pentagon Papers.

---

3. Exploit technology.

(https://fightgangstalking.files.wordpress.com/2013/05/technology.jpg)

Technical counter-measures can seriously disrupt some forms of surveillance and harassment used in organized stalking.

If you can afford to buy counter-surveillance and security equipment (cameras, alarm systems, locks, safes, firearms, bug detectors, signal jammers, etc.), you should do so.

Be as discrete as possible about acquiring and implementing such measures so as not to make them easier for your stalkers to defeat. If possible, try to have friends or relatives make the arrangements and purchases, since they are less likely to be under constant surveillance.

Using technical security measures to fight gang stalking has two major limitations though.

One is the cost. Most targeted individuals lack the financial assets to take advantage of many security technologies; people with significant resources and connections are probably not often selected as gang stalking targets in the first place since they can more easily fight back.

The other problem with a strategy that relies primarily on technical counter-measures is that you will essentially be engaged in a sort of "arms race" with people who have a deeper knowledge of such matters, as well as deeper pockets.

Nevertheless, it is smart to exploit spy gear and security systems as much as possible within your budget. Some effective technological counter-measures are either free or relatively affordable. I try to address those in the sections below.

---

4. Never give up.

(https://fightgangstalking.files.wordpress.com/2013/05/winston-churchill-quote-keep-going1.jpg)

Persistence will lead to victory. Already the digital public square is filled with information and rhetoric which the U.S. government would prefer to censor but cannot, posted by Americans fed-up with the corruption, secrecy, and abuses of power in the upper echelons of government and corporations.

Even the federal government's massive self-serving security apparatus and its abettors in mainstream media institutions cannot effectively monitor and control the flow of information anymore. Dissent is harder to marginalize and censor in a digital landscape filled with whistle-blowers, citizen-journalists, bloggers, and alternative media websites (from all across the ideological spectrum).

Independent thinkers, entrepreneurs, entities such as *WikiLeaks*, and movements such as *Anonymous* have created an information network in which citizens no longer have to wait for the *New York Times* to expose the next Pentagon Papers conspiracy – or the *Washington Post* to expose the next Watergate scandal. Even the *New York Times* admits this:

"News no longer needs the permission of traditional gatekeepers to break through. Scoops can now come from all corners of the media map and find an audience just by virtue of what they reveal." – David Carr, *New York Times*, June 16, 2013

One of the objectives of gang stalking is to isolate and break-down the targeted individual by creating the impression that the whole society is against him or her. Don't make the mistake of believing that false impression. Although the number of people who participate in gang stalking must be large, they are still a very small minority compared with the general population. The vast majority of Americans do not wish to have our society become a creepy police state filled with citizen spies, as happened in the communist nation of East Germany.

Gang stalking victims need to challenge the careerist statist rodents in the food chain, and support political reformers – libertarians, progressives, and others – who defend the individual rights and freedoms of Americans against the predatory inclinations of powerful government and corporate institutions.

---

5. Join forces with other victims.

(https://fightgangstalking.files.wordpress.com/2013/05/join-forces-chain1.jpg)

Join forces with other gang stalking victims by concentrating on just a few online platforms to share information and expose gang stalking.

Not only are gang stalking victims often in various stages of financial ruin because of their enemies, and short of contacts because of their isolation, they also don't have one clear source to which they can go for information and support.

African-Americans have the NAACP; American Muslims have CAIR (Council on American-Islamic Relations). If members of those communities are looking for advocacy, they know where to go.

Targets of gang stalking in contrast are isolated individuals with numerous scattered, marginally-useful websites to go to for information, and those are mixed in among search results with numerous disinformation websites created by government minions.

To have any hope of ever gaining the attention of Congress, targeted individuals must at least begin coalescing around just a few major information sources. This website is intended to be one of those.

For every legitimate anti-gang-stalking website, there seems to be a dozen which are mostly or completely filled with garbage. Every gang stalking victim who has searched for information online knows this is true.

As you visit websites which appear in searches about gang stalking, you first see something which appears to be a possible source of useful information, but on closer look is just a lot of vague B.S. mixed with UFO abduction story links or whatever.

I have listed some of the few exceptions in the "Recommended Websites" page of this blog. There are other legitimate sources as well, but not many.

Consequently, anyone (who is not a targeted individual) searching online – for example, a journalist – will mostly encounter what appears to be evidence that gang stalking is the product of the imaginations of paranoid and mentally-challenged individuals.

Merely creating one more blog or Facebook page to get lost in the ocean of such information is not going to solve the problem. If you want to create an anti-gang stalking website, blog or Facebook page, by all means go ahead (in fact I encourage it), but you should seriously consider also trying to help the community of gang stalking victims coalesce around a few locations – instead of existing only as isolated points spread across the web in a sea of

disinformation.

Toward that end, I humbly suggest that you try to promote this website – FightGangStalking.com – as a comprehensive source to which people can go. This suggestion might seem self-serving, but you can see for yourself that I'm not making any money from this website: there's nothing for sale here.

I will continue attempting to publicize the best suggestions, websites, articles, video links, etc. about gang stalking as they come to my attention by listing them in this website.

Instead of having each victim of gang stalking re-invent the wheel and create a website which attempts to explain gang stalking from scratch, consider creating a more limited website, Facebook page, or blog, which describes your experiences with gang stalking, but also prominently features a link to this website.

As mentioned above, another thing that would be helpful is to go online and post comments in other websites, forums, Facebook pages, Twitter messages, emails, etc.) referring people to this site.

As much as possible, you should do that both at gang stalking websites and in the comments sections beneath articles in major news websites, so they will be seen by non-victims of gang stalking as well. That's critical.

One very easy way to post such information is to simply copy information from this website – if it relates to an article or a forum discussion.

The best way to connect with other victims of gang stalking is online – although you must beware of perps who pose as targeted individuals (see the "FFCHS" page of this website for details). In general, be suspicious of anyone reluctant to publicly criticize the apparent participation in gang stalking by law enforcement officials.

The very best thing would be for victims to create a legitimate victims' support group to lobby for the exposure and elimination of gang stalking by petitions and public demonstrations.

If any particularly ambitious gang stalking victim wishes to spearhead an effort to form such a group, please email me about it so I can promote it here. Even though it would inevitably be infiltrated by some perps, it could still be very effective.

(https://fightgangstalking.files.wordpress.com/2013/05/blue-line3.jpg)

B. Tradecraft

I am using this term somewhat loosely here; from the perspective of anyone targeted by America's Stasi, everything on this webpage is our "tradecraft." Traditionally, the term refers to the set of specialized methods used by intelligence and counterintelligence agents.

1. Fortification

(https://fightgangstalking.files.wordpress.com/2013/05/neuschwanstein_castle.jpg)

Although it is impossible to make your residence completely secure against all potential threats, you can make it far more risky for intruders by taking certain precautions.

A full discussion of home security concepts and hardware is beyond the scope of this website. I will mention a few principles here – and try to add more information in the future – but I encourage you to invest some time reading more about this subject and exploiting established security practices and technology.

Here is an example of some good basic advice on this topic. (http://www.townofwoodway.com/documents/BurgTips2.pdf)

Begin by implementing standard basic security measures.

Secure all your windows from the inside with bolt locks, and test them from the outside to ensure integrity.

If you have multiple entrance doors, secure all but one of them from the inside with bolt locks before departing, so as to restrict access to a single door.

Install a simple, self-contained alarm system on the entrance door. Arguably, a simpler system will be more difficult for stalkers to defeat than a more expensive sophisticated remotely-monitored system.

Advances in digital audio and video recording devices are making surveillance cameras better and more affordable all the time. Install several small cameras to monitor the entrance from different angles.

Think creatively about how you might arrange for some unpleasant surprises to occur for anyone who visits your residence uninvited while you are not home.

Various laws could apply depending upon the country and region where you reside, but if you determine that it is legally appropriate to implement certain arrangements that are physically dangerous for intruders, that would certainly create some interesting options.

Those options could be very cheap and low-tech also – perfect for asymmetrical warfare. If you can develop a fool-proof system for not endangering yourself and other innocent people, you might want to consider, for example, the potential of strategically duct-taping razor blades to various places in and around your residence. Creatively-placed fish hooks, needles and broken glass can also make your residence less friendly to criminal intruders.

---

2. Disappearing

(https://fightgangstalking.files.wordpress.com/2013/05/disappearing.jpg)

Performing a "cleaning run"

For most individuals targeted by organized stalking, it is probably not practical to invest a lot of time trying to master the "tradecraft" of the intelligence and security industry; however, it is worth taking a look at some of the concepts.

In the spying business, a "cleaning run" is a process by which an individual who is the target of surveillance, escapes that surveillance – at least temporarily – by traveling on an unpredictable route over a period of several hours, using a series of different means of transportation and exploiting a variety of environments (busy intersections, deserted areas, underground parking structures with multiple entrances and exits, etc.).

Obviously, such a run would also require abandoning things which can be tracked by GPS monitoring, such as a personal vehicle. If you are carrying a cell phone, you need to remove the battery. (https://ssd.eff.org/wire/protect/cell-tracking) That is the only way to ensure it is not being tracked. (Merely turning off the power will not work.)

Some elements of cleaning runs are technical, but most of it is common sense. The targeted individual needs to have a detailed plan, but also needs to create that plan discretely.

Obviously, for most targeted individuals, cleaning runs are mostly only viable as a short-term way to get off of the radar. A long-term solution would require the ability to live somewhere anonymously – a much bigger challenge – especially in an age of ubiquitous electronic record keeping, surveillance cameras and such.

It is far more realistic to work at exposing the deep corruption in America's law enforcement and intelligence agencies. That can lead to political efforts to rein-in the rodents who profit from the surveillance state. Targeted individuals should take their inspiration from patriots like Edward Snowden.

Here are a few websites which give you a very basic idea of what cleaning runs are about:

http://nymarketing.wordpress.com/2011/05/16/counter-surveillance-the-cleaning-run-and-evading-capture/ (http://nymarketing.wordpress.com/2011/05/16/counter-surveillance-the-cleaning-run-and-evading-capture/)

http://www.spytrainer.com/Articles/Art_Cleaning.htm (http://www.spytrainer.com/Articles/Art_Cleaning.htm)

For a deeper look into these kinds of tactics, you might want to purchase a book such as this one: *Surveillance Countermeasures (http://www.amazon.com/Surveillance-Countermeasures-Serious-Detecting-Personal/dp/0873647637/ref=pd_sim_sbs_b_7)*

_____

"How To Disappear: 9 Ways To Avoid The Creepy Surveillance Systems All Around You"

This article (http://www.huffingtonpost.com/2012/09/18/how-to-disappear-avoid-surveillance_n_1872419.html) gives an idea of the kinds of gadgets available to help you stay under the radar.

---

3. Computer & Phone Security

(https://fightgangstalking.files.wordpress.com/2013/05/computer-security.jpg)

Corrupt current and former agents of intelligence and law enforcement agencies and their corporate clients will almost always have more financial and technical resources than the individuals they're stalking. So despite your best efforts, it will be difficult to achieve full computer and phone security.

Therefore you should never assume that your electronic communications have not been compromised. For information that needs to be completely secure, you will need to rely upon non-electronic means – face-to-face communication in remote unpredictable locations, hand-written notes (or a typewriter) to record information, etc.

On the other hand, you can sometimes at least make electronic spying difficult for stalkers by using certain technical counter-measures, such as encryption. Electronic security is very much like the physical security of your home: a determined and skilled burglar can get into your house despite your security precautions, but it still makes sense to lock your front door. Similarly, you might never make your electronic data completely unreachable, but it still makes sense to protect your information as much as you can.

Anonymous Web Browsing

If you want to browse the Internet relatively anonymously (for example, as you search for gang stalking and counter-surveillance information), you can download and use the free web-browser called ***Tor*** (https://www.torproject.org/). (https://www.torproject.org/)

Internet browsing via the Tor network is relatively secure, but it is also very slow. For most of your regular non-sensitive Internet activity you might want to use Mozilla's popular free open-source ***Firefox*** *(http://www.mozilla.org/en-US/firefox/new/)*browser, which is generally rated highly for security.

Note: For whatever reason, the Firefox browser seems to clash with the blog template I use for this website. I recommend that you use Google Chrome or Internet Explorer instead when visiting Fight Gang Stalking.

Operating systems that can be booted from your flash drive

To further enhance your anonymity, you can use an operating system called ***Tails*** (https://tails.boum.org/about/index.en.html), (https://tails.boum.org/about/index.en.html) which is designed to work with the Tor network. It will work with almost any computer, and can be launched from a USB flash drive, DVD, or SD card. Your files are encrypted and your activity leaves no trace on the computer.

Anonymous Search Engines

If you wish to avoid using Google as your search engine – since, for example, one of its chairmen was apparently a friend of the war criminal Henry Kissinger (see June 1, 2013 entry in "Gang Stalking News" section of this website), you can instead use a search engine called ***Start Page*** (https://www.startpage.com/) – which is specifically designed to be more anonymous. They bill themselves as "The world's most private search engine."

Another search engine which does not track its users is ***DuckDuckGo. (https://duckduckgo.com/)***

Internet Search Techniques

Even though most search engine queries are simple, if you want to dig more deeply into the information available online, it is worth learning more about research tools and strategies. This booklet is a bit dated – it was created in 2007 – but it will help you sharpen your skills for exploring the Internet.
Untangling the Web (https://fightgangstalking.files.wordpress.com/2013/05/untangling-the-web.pdf)

Encrypted Email

If you want to encrypt your communications – such as emails – you can use a program called ***Pretty Good Privacy (PGP). (https://en.wikipedia.org/wiki/Pretty_Good_Privacy)***

The simplest way to exploit the advantages of Pretty Good Privacy encryption is to use the free email service called ***Hushmail*** (https://www.hushmail.com/). (https://www.hushmail.com/)You can set up a free account in about two minutes.

You will need to also have your friends and relatives create Hushmail accounts. When emails are exchanged between two users of Hushmail, the contents are automatically encrypted. Of course, Big Brother's vast army of mathematicians and hackers at the NSA presumably have little trouble defeating such security in various ways, but it's better to at least make the effort to be as secure as possible. You can set up a free account at Hushmail.com. The only drawback to (the free version of) their service is that you must log-in at least once every three weeks to keep it active.

Another reputable free email service which uses encryption is ***Riseup.*** (https://help.riseup.net/en) They also offer other secure communication services, such as voice and video chat and Virtual Private Networks (VPN).

Testing your computer's firewall

Gibson Research (https://www.grc.com/x/ne.dll?bh0bkyd2) is a well-established source of information (and software) regarding computer security. At their website you can test the security of your computer's firewall. Visit their website and scroll-down to the bottom of the page and click "Proceed." On the next page, click the button that says "GRC's Instant UPnP Exposure Test."

Ad-Blocking Applications

(https://fightgangstalking.files.wordpress.com/2013/05/online-stalking.jpg)

As you probably know, most online advertisements are targeted – as much as possible – toward particular consumers based on data about them. For example, if you perform a Google search for a particular product or service, you are likely to begin seeing pop-up ads related to that subject.

Sometimes gang stalkers exploit this by targeting your computer's IP address and online accounts with ads specifically intended to harass you.

At one point the local gang stalking crew in my neighborhood began dropping life insurance brochures on the walkway to my door inside my courtyard. Then they followed up with a barrage of Internet ads about life insurance – just to drive the point home. It was a classic "no fingerprints" form of gang stalking threat, because it's difficult to persuade others (let alone prove) that the brochures and ads are not simply coincidental. The threat was reinforced with the online ad shown above – ostensibly an ad for a novel.

You can eliminate most – but not all – pop-up ads by downloading
an ad-blocking application. Among the best of these programs is
Ad Muncher (http://www.admuncher.com/), which is now available for free.

Electronic Frontier Foundation (EFF)

For a more comprehensive look at how to protect your computer from Big Brother's surveillance, you can refer to this guide (https://ssd.eff.org/) by the non-profit Electronic Frontier Foundation (EFF).

Electronic Privacy Information Center (EPIC)

Another reputable non-profit organization that fights against anti-American spying on computer activities is the Electronic Privacy Information Center (EPIC). This page (https://epic.org/privacy/tools.html)of their website lists some recommended privacy tools.

Encrypted smart phones

Some phones offer encrypted voice calls and text messages. This *PC Magazine* article (http://www.pcmag.com/article2/0,2817,2454563,00.asp) from March 2014 gives you an idea of what is available.

Face-to-Face Communication

Every form of electronic communication can potentially be compromised. If you are discussing matters you wish to keep private, face-to-face conversation should be used instead whenever possible. Go outside and find an unpredictable location for your discussion.

Privacy for indoor conversations can be greatly enhanced by using the effect of "white noise." One way to do this is to stand close to a sink, turn on the water full-blast, and speak quietly. It can be nearly impossible to detect conversation in that situation.

---

4. Spy Gear

(https://fightgangstalking.files.wordpress.com/2013/05/spy_vs_spy___by_mario_bordieri_by_bordieri.jpg)

Artist: Mario Bordiari

Products Available

I have no personal knowledge of this particular company (http://www.brickhousesecurity.com/category/counter+surveillance.do), but it seems to offer a wide range of products, so this will give you an idea of what is on the market. It is mostly obvious how the devices featured could be used to document or disrupt the activities of the criminals who perpetrate organized stalking.

Bug Detectors

From my brief online survey of bug detection (camera and microphone detection) hardware, it seems that detectors range from about $80 for basic portable devices to about $2,700 for professional-grade state-of-the-art equipment. The obvious question is: How much do you need to spend to obtain gear you can have confidence in? That is difficult to say because distributors (who presumably have the most expertise) also have an incentive to sell you the priciest gear.

The following is just some basic information I plagiarized from various online sources. My thanks and apologies to whoever wrote it. Technology information should be frequently updated of course, but this is fairly general advice.

Purchase a counter-surveillance device that can detect the magnetic fields and electrical "noise" produced by computer circuitry. Many surveillance cameras and audio bugs emit radio waves and can be identified by a standard RF (radio frequency) detection device.

Conduct a "sweep" of your home with your bug detector. Surveillance devices are often hidden in walls or ceilings, so look for any spots that appear to be spackled or recently spackled. However, with the decreasing size of surveillance equipment, they can be concealed virtually anywhere. Household objects such as pens, clocks, lamps and even watches may contain devices to see and hear what you are doing.

Repeat sweeps frequently. Many surveillance devices can switch frequencies or shut on or off to avoid standard detection equipment. And, of course, a device might simply have a dead battery (until someone replaces it).

Small bug detectors might be used to track audio bugs in the phones or near the phones. Larger bug trackers, measuring the size of a briefcase, can track spy cameras, audio spy equipment and have much more functions than smaller ones. Of course, such detectors cost more also.

More advanced bug detectors not only allow you to detect any bugs in the room, they can also "steal" the RF signal and display what the security camera sees. If the CCTV cameras don't use any signal encoding, then such spy cam bug detectors will easily display you the wireless camera's view.

How a Bug Detector Works

Wireless devices, like spy cameras or even computer networks, work by sending radio signals from one location to another. Such signals are called RF, which refers to "Radio Frequency". Such devices use RF signals to communicate with the receivers. Now a bug detector simply scans the whole room or office for such radio signals and reports to you when it detects anything.

One note here. If you're doing surveillance in your house, then turning off some wireless devices, like cell phones could be a good idea. This is just to help you better track and spot bugs or spy cameras in the room.

Frequency Range

Usually, bug detectors operate in 2 GHz or 3 GHz frequency range. Now, most spy devices also operate in this range, so there are no problems spotting a bug in that range. However, some (more sophisticated) spies will change the frequency of a bug to a higher level, like 4 GHz or 6 GHz. Then, a common bug tracking device won't be able to catch any frequencies, but a more advanced solution will do the job.

There are powerful bug detectors for private investigators; or the ones that police use, which can detect RF signals even up to 9 GHz. They cost more, but they'll spot any bug in the room without problems.

Can Surveillance Bugs Spot Wired CCTV Cameras?

Most bug detectors are able to track almost any wireless spy device that uses RF signals – whether it is a wireless mini hidden camera, a phone bug, or a blue tooth spy cam…

But, detecting hard-wired cameras was a little problem. It's simply because they don't use radio frequency signals to transmit data between the transmitter and a receiver. Now, powerful bug tracking devices can spot even wired CCTV cameras in the area.

(https://fightgangstalking.files.wordpress.com/2013/05/blue-line3.jpg)

C. Interacting with Perps

1. Scripted Responses & Fake Phone Calls

(https://fightgangstalking.files.wordpress.com/2013/05/jack-webb-reading-script-on-set.png)Use the tactics of your enemies when they are useful for your purposes.
(https://fightgangstalking.files.wordpress.com/2013/05/jack-webb-reading-script-on-set.png)

Lower-level perpetrators of the direct face-to-face harassment involved in organized stalking almost always interact with the targeted individual in a tightly scripted way. The perpetrator is directed to make a specific comment and/or perform a specific action based upon the particular victim and circumstances.

This is done for a very good reason. It allows the handlers to control the harassment in ways which follow a thoroughly tested playbook that has been developed and honed over years of psychological operations by the Stasi, the FBI, and other counterintelligence agencies.

Comments are intended to be as creepy and insulting and provocative as possible (and tailored to the individual victim as much as possible) without including any language that might be incriminating or legally objectionable or suspicious in case they are recorded.

Similarly, the perpetrators' actions – such as cutting the victim off or brushing against him – are chosen because they will not appear extraordinary to outside observers. (People do sometimes brush against other pedestrians or cut them off – either accidentally or because of common rudeness.) If the actions are witnessed or captured on video, they will seem inconsequential – especially when viewed as an isolated act.

The point is that few, if any, of these acts of harassment are spontaneous, which reduces the chances of mistakes. That logic can be used by targets of gang stalking also. Instead of simply reacting to each act of harassment impulsively when baited by the perpetrators, it is better to have a standard phrase and course of action mapped-out in advance.

This is true both for "street theater" public harassment and the "mobbing" in the workplace by co-workers. If you have a standard action and phrase to use (one which you have mentally rehearsed and chosen for its lack of potentially incriminating language) you will not be forced to respond on impulse.

Sometimes gang stalking perps try to bait targets to react in ways that they can document and use against them (a classic FBI trick). Don't give them anything to work with. When they say or do something insulting, you should respond based on your plan.

Responding to Harassment in the Workplace

If you're being mobbed (verbally harassed in your workplace), consider responding to every single instance of such harassment by saying something like *"I read that people who engage in workplace mobbing are all brown-nosers. Do you think that's true?"*

If they try to draw you into a discussion about that – for example, by saying *"What do you mean?"* just smile and say *"I just thought that was an interesting theory."*

Always say that. Don't ever say anything else. Your co-workers will grow tired of having you respond to their insults by hearing you re-ask for the twentieth time whether they think perpetrators of workplace mobbing are all brown-nosers, and having you refuse to get drawn in beyond commenting that you think that's an interesting theory.

And those exchanges are not the type which employees and managers will want documented verbatim in human resources reports.

An alternate choice of words you might want to adopt as your default comment would be this: *"You've got a little bit of brown stuff on your nose."*

That is taking a page out of the playbook of the Stasi goons. It will annoy the perp because it will be true – *and they will know it is true.* That is the kind of thing that gets under a person's skin.

Also – what are they going to do about it? They could secretly record what you are saying perhaps, but that would just support your claim that you are being systematically spied upon.

A taste of their own medicine. 🙂

Responding to Harassment in Public – Fake Phone Calls

When you are at work, there are limits to what you can say out loud to gang stalking perps without creating problems for yourself. That does not apply to most other situations. Whenever you encounter a stalker (or even someone you think could ***possibly*** be a stalker) anywhere outside of your workplace, this is how you should respond:

Place your cell phone to your ear – as if you are having a phone conversation. If you don't have a cell phone handy, just cup your hand to your ear as if you were holding a small cell phone – it does not need to be convincing. Then stare right at the perp and smile and say – ***very loudly*** – something crude and insulting.

Use your imagination (in advance) to come up with one standard crude insulting phrase that could always be used. Just make sure it's very crude and very insulting. Gang stalking – like politics – "ain't bean-bag."

Something along the lines of *"They sent another brown-noser!"* would be appropriate. If you can think of something worse, that's even better. Just refrain from *threats* – since that could get you into legal trouble.

Repeat as needed. If you get no response, say it again – even more loudly: *"I **said**: They sent another brown-noser!"* Always keep smiling as you say it and keep looking directly at the perp.

In between insults, you might wish to say this – for the benefit of anyone other than the perp who might be in the vicinity: *"My cell phone has a terrible connection. I'll try to talk louder."*

If the perp is walking away from you without responding, shout to him or her in the same tone of voice used when you're trying to get the attention of someone who has dropped something and does not realize it: *"Hey! Hey! Brown-noser!"*

Push this as far as you like. Perps are kept on a very short leash, so to speak, by their handlers. They know that if they respond physically, they will get into big trouble with the Stasi agent who tells them what to do. I know this – I have field-tested the theory. 🙂

You get the idea. The important thing is to rehearse this mentally in advance so you will react immediately each time without having to think about it at all.

Keep it simple. Don't try to be Oscar Wilde. Gang stalking perps are often just just a notch or two above mental retardation. You need to connect with them on their level.

If you are not sure whether someone is a perp, go ahead and still use the tactic anyway – just to be on the safe side. If the person is not a perp, he or she will just think you are a loud obnoxious jerk having a crude cell phone conversation with someone. That isn't really an uncommon event these days, and it is not illegal either.

Note that this fake phone call tactic can also be used effectively in the workplace – although you might want to invest slightly more effort to seem convincing about actually making a cell phone call in case you're in the vicinity of employees who are not directly involved in the harassment (or surveillance cameras).

---

2. Taking Photos & Videos of Stalkers

(https://fightgangstalking.files.wordpress.com/2013/05/dsc00513-cropped.jpg)

Based on my own experience and accounts of other targeted individuals, perps don't like being photographed when they're stalking you. Some will be more bothered by it more than others, but none of them will want you to do it.

With the variety of digital cameras available (cell phones, spy cameras, etc.), you can take photos and videos either overtly or covertly. Both have advantages. If you are trying to annoy the perp's, taking their photo in an obvious way, might be a good method. On the other hand, if you're trying to document their actions, a covert spy-camera approach might be better.

Of course, it's unlikely that your photos and videos will have much legal significance. Perps are told to avoid doing and saying things that could be incriminating. They are normally following very specific directions from their handlers – for example, they are told to make a comment which is not explicitly threatening or slanderous, but which makes reference to something they know about you from conducting illegal surveillance.

I encourage stalking victims to post the clearest photos of the perps online. Try to get good close-up clear shots of their faces. Obviously, the above photo is not a good example of that – although it is a photo of someone who seemed creepy and suspicious in front of my residence at a time when that block was infested with gang stalking perps.

Don't post photos in a way that could be considered libelous. For example, don't write a caption which says "These are my stalkers." Instead, say something like "Here are some people I have seen near my residence, where I'm being gang stalked. Maybe one of these people witnessed something that could be helpful." 🙂

A note about your legal rights to take photos and videos:

If you are in a public space, you have the right to photograph anyone (or anything) in plain view. When you are on private property, the property owner may establish rules about taking photos.

For a full discussion about your rights as a photographer, see this ACLU web page. (http://www.aclu.org/free-speech/know-your-rights-photographers)

---

3. Making Noise

(https://fightgangstalking.files.wordpress.com/2013/05/air-horn.jpg)

Harassment by noise is one of the most common tactics of gang stalkers. Now it's your turn to exploit noise: buy an ***air-horn***. They're cheap (they start at about $15). If you live near a store that sells boating supplies, you can get one there. Otherwise you can order one online.

Carry it with you if you're encountering perp's on the street in your neighborhood. Use it like a rape whistle. The next time someone makes some creepy comment, take it out and blast it for a few seconds. You should probably use some ear plugs though; air-horns are *loud*.

Just smile at the perp while you're doing it. If anyone asks, tell them the truth: you're being gang-stalked. Simple as that. If the perp asks you what you're doing, say "Stop gang-stalking me." Of course, you should say it in a friendly voice and smile while saying it. You might have to speak loudly though; his ears might be ringing.

It's possible that someone could complain that you're disturbing the peace, but it's very unlikely that local cops (who will know about gang stalking) will want to make an issue of it.

By the way, this isn't just a theoretical tactic; I tested it. 🙂

---

4. Suppressing Noise

(https://fightgangstalking.files.wordpress.com/2013/05/anti-noise-headphones.jpg)

Since harassment by noise is one of the major tactics of gang stalkers, you might want to purchase a pair of ***noise-cancelling headphones*** (http://reviews.cnet.com/best-noise-canceling-headphones/) ($80 to $400).

If you cannot afford them, you might want to buy some disposable ear plugs. They will also be handy if you decide to use the air-horn tactic described above.

---

5. Always Smile at the Goon Squad

(https://fightgangstalking.files.wordpress.com/2013/05/smiling-shark.jpg)

Exploit this common valuable advice of anonymous origin:

"Smile. It makes people wonder what you're up to."

Every time you see someone who could even possibly be a member of the local gang stalking goon squad, you should greet him or her with a big grin. Every time. Stare right at the idiot and smile.

Even better is to combine this with the tactic explained previously – "Use scripted responses" – by initiating a fake cell phone conversation as a pretense for mocking the perp with crude insults.

But you should always smile at the perp. Although the "street-level" stalkers are generally the stupidest of the various minions, even they are smart enough to understand that the goal of their efforts is to emotionally destroy their target.

Make it clear to them that they are failures. 🙂

---

6. When is it Appropriate to *Kill* a Stalker?

(https://fightgangstalking.files.wordpress.com/2013/05/sw-357.png)

I hope I am not alienating potential allies by touching on a subject as controversial as firearms, but a discussion about "tactics for fighting back" would be incomplete without some reference to this issue.

Since I am not a lawyer, I do not offer legal counsel. Also, the particular circumstances of any situation can have important legal implications, so I would not try to give general advice about when it might be legally defensible to kill a particular criminal who is threatening you. I will simply make this layman's observation: if you are defending yourself – for example, using the very concealable and very powerful Smith & Wesson .357 Magnum pistol shown above – you should do so in accordance with the various municipal, state, and federal laws that apply.

Also, it might be productive to clearly communicate in various ways – in advance – to any local criminal conspirators (professional and volunteer) your willingness to defend yourself.

Specific advice on firearms is beyond the scope of this website, so – for example – I will not attempt to wade into the debate among experts about the relative merits of handguns-versus-shotguns for home defense, but here are some primers on the basics of firing and cleaning handguns:

- Fundamentals of Handgun Shooting (https://fightgangstalking.files.wordpress.com/2013/05/fundamentals-of-handgun-shooting.pdf)
- Cleaning Handguns (https://fightgangstalking.files.wordpress.com/2013/05/cleaning-handguns.pdf)

Since firearms regulations vary across different states and municipalities, I will not try to generalize about the advisability of particular tactics.

One can imagine though, some of the ways individuals targeted by illegal harassment might respond with firearms. In a society as well-armed as the U.S., the potential for violence is obvious. This reveals much about the priorities of the DOJ and FBI, who apparently sanction psychological operations harassment despite the obvious danger of retaliatory violence against neighbors of the victim.

Perhaps illegal criminal harassment as a counterintelligence weapon is not actually sanctioned by the federal government. You just have to guess about that. For some reason, law enforcement officials never publicly discuss the issue.

Persons targeted by illegal surveillance inside their own residences might decide to do some "targeting" of their own. For example, they might occasionally point loaded firearms at the residence(s) used by those conducting the illegal surveillance.

A targeted individual might even shoot at the perpetrators – although merely *pointing* a loaded weapon at the perpetrators frequently (with the safety mechanism disengaged) could give them something to think about, since there would always be the possibility of an accident or whatever.

Such counter-measures would probably be especially tempting to use if the firearm was of a sufficiently high caliber to easily penetrate walls.

Obviously, targeted individuals would probably not do that sort of thing with the blinds open – in plain view of persons who were outdoors and could capture such behavior on camera.

I would guess that victims of gang stalking might want to make occasional trips to a firing range to refresh their skills and to confirm that no one had tampered with their firearms during a black bag operation.

Of course, I am not advocating any of this. I am just speculating about how an individual might be likely to respond to organized stalking by corrupt law enforcement and intelligence agencies.

(https://fightgangstalking.files.wordpress.com/2013/05/blue-line3.jpg)

D. Exposing the Perps Locally

Lobbing a Grenade into the Rats' Nest

(https://fightgangstalking.files.wordpress.com/2013/05/hand-grenade.jpg)

I apologize, incidentally, for the apparent inconsistency of referring to America's brown-nosed Stasi brigade, variously as "cockroaches" and as "rats." In my defense though, the taxonomy of their tribe is a bit complicated – as I make clear on the "What is Gang Stalking?" page of this website.

Our strategy for pest control is a bit simpler; it consists of two main elements.

This a two-front war. We must act locally to expose the perps to neighbors and others – for example by mailing flyers, as explained below. At the same time we must also try to expose what is happening on a national level – which I address in the next section. Both elements are critical to success.

Here are some tactics for disrupting the activities of the local rodent population. Gang-stalking perps try to conduct their operations as quietly as possible and maintain a low profile. We should mess that all up. 🙂

1. Emails & Letters to Local Officials & Organizations

(https://fightgangstalking.files.wordpress.com/2013/05/email-to-local-officials.jpg)

In at least some cases, perps operate with the direct cooperation of local law enforcement – or at least with their passive acquiesence. Presumably, in some cases, various local officials and other professionals are also "in the know" about gang stalking crimes, but they will not want to discuss it openly.

Here is how you shake things up:

(1) Visit the websites of your local city and county government offices and make a list of every email address you can find – from the park maintenance staff to the mayor and county officials.

(2) Download either the flyer in the section immediately below or the letter posted in the section on letters to Congress (that letter is also posted in the last section of this webpage).

(3) Highlight and copy the text and paste it into the body of an email and address it to everyone on your list.

Note: You will probably want to send the email from an anonymous email address, although what you are doing is legal, so you don't need to worry about it being traced.

(4) Send your email. You will have established the watercooler discussion topic for the day. 🙂

---

2. Flyers

(https://fightgangstalking.files.wordpress.com/2013/05/flyer-distributor.jpg)

Distributing flyers is probably the single most powerful tactic for fighting back against America's Stasi goon squads. Mailing flyers anonymously – or placing them on walkways or doorsteps of residences – is a legal, simple, cheap, and very effective way to expose the crime of organized stalking. Counterintelligence perps do not have a good way to suppress this particular avenue of communication. Also, this tactic circumvents the problem of cowardice and laziness in the mainstream corporate news media because it exposes the information directly to the public.

Using pamphlets to criticize stupidity and corruption is a deep tradition which includes legendary thinkers and activists such as Thomas Paine (http://en.wikipedia.org/wiki/Thomas_Paine) and Lysander Spooner. (http://en.wikipedia.org/wiki/Lysander_Spooner) Even in an age of television and the Internet, pamphlets remain a powerful communication weapon to expose crimes by government officials. In fact, they are much more powerful in the digital age precisely because they can refer readers to websites (such as this one) for additional information.

An HBO documentary called *Mea Maxima Culpa* chronicled the sexual abuse of boys by a priest at a school for the deaf in the 1950s and '60s. When the victims could not get help from authorities, some of them began distributing flyers which identified their abuser. It was a desperate tactic, but not without effect. Although the perpetrator was never prosecuted, his exposure ultimately forced him into retirement.

You will accomplish multiple objectives by distributing flyers: (a) your neighbors will have some clue about what is happening – which could force the local street-level perpetrators to limit their harassment somewhat, (b) the local police will be forced to contend with some inconvenient questions from citizens about what is happening, (c) the (non-cowardly) members of the news media might investigate and report on it, and (d) such reporting could create pressure for members of Congress to acknowledge the reality of organized stalking – and perhaps initiate an investigation – as was done by the U.S. Senate's Church Committee during the 1970s regarding the FBI's infamous Cointelpro operations and the CIA's Project MK Ultra.

In 2009 Frank L. Raffaele, a resident of Verona, New Jersey was targeted by gang stalkers, and he responded by distributing flyers about the harassment to neighbors and businesses. The flyers generated enough discussion and inquiries that the local police were forced to address the issue, and it became the subject of an article in the local newspaper. (https://fightgangstalking.com/#newjerseyflyers)

In July 2014, a victim of organized stalking in Guilford, Connecticut distributed flyers to great effect. This was a perfect example of the power of this tactic. A local TV news report on WTNH News 8 (//wtnh.com/2014/07/04/flyers-threatening-gang-stalking-scaring-people-in-guilford/)and a local TV news report on an NBC News affiliate, and an article in the Connecticut newspaper, *The Courant*, reported that hundreds of "suspicious flyers" about "gang stalking" were being distributed. The flyers made reference to this website (Fight Gang Stalking), and alleged that organized counterintelligence stalking was being perpetrated in Guilford. A statement by the Guilford Police Department about the matter was also posted in *The Day* newspaper. A copy of one of the flyers was posted on *The Courant's* website. ***Final score: targeted individuals 10, security industry parasites 0.*** 🙂

If you can afford the postage, *mail* your flyers.
(https://fightgangstalking.com/#newjerseyflyers)
Send them to residences, businesses, and schools in your neighborhood as well as to local officials.

I recommend that you send your flyers anonymously. You are encouraged – but not legally required (https://en.wikipedia.org/wiki/Return_address) – to include to include a return address on your envelopes. You also do not need to address the envelopes to the residents by name; you can simply address them to "Resident."

If you do want to address flyers to your neighbors by their names, you can go to a website such as WhitePages (http://www.whitepages.com/) to find the name(s) for each address. Just click on the "Reverse Address" search tab.

Be as discrete as possible when mailing the flyers. Ideally, have a friend or relative do it so it will be more difficult for the perpetrators to intercept and disrupt the mailing (for example, if they have an accomplice at the post office). It is unlikely that they would interfere with such a mailing though, as it would be a serious violation of federal law.

Distributing your flyers directly

If you cannot afford the postage to mail your flyers, you should distribute them by going door-to-door. You do not need to speak with residents directly; just leave your flyers where they will be seen. This tactic is completely legal by the way. If it is legal for the KKK to leave flyers on peoples cars, doorsteps, and front yards (and apparently it is), (http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10735377/Ku-Klux-Klan-on-new-recruitment-drive-with-leaflet-drop-in-towns-across-America.html) then it is legal for you to do so.

One of the few restrictions is that you are not allowed to place flyers inside mailboxes – or even touching mailboxes. (http://www.cleveland.com/business/index.ssf/2010/04/postal_service_controls_the_ou.html)

I suggest you go to a print shop or office supply store and have your flyers printed in large numbers at a low cost. That beats wasting money on personal computer printer ink.

Purchase the best quality of paper you can afford. The documents will be taken more seriously if they are printed on quality stock.

Be provocative; your flyers need to be noticed. Consider using a red marker to soak some ink blotches onto your flyers that will resemble blood drops.

The flyer below refers to anti-stalking laws in California. If you live in another state, you can just change the criminal code references to match the stalking laws in your state's criminal code. This website conveniently lists the criminal code sections for the stalking laws in each state. (http://www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-laws/criminal-stalking-laws-by-state)

You will also need to change the state and phone number reference for your state's attorney general.

Click on Image to Enlarge

(https://fightgangstalking.files.wordpress.com/2013/05/gang-stalking-flyer1.jpg)

To download this flyer as a Word document click here:

Gang Stalking Flyer (https://fightgangstalking.files.wordpress.com/2013/05/gang-stalking-flyer3.docx)

Here is another flyer you might find helpful to stir things up:

Click on image to enlarge:

(https://fightgangstalking.files.wordpress.com/2013/05/jean-seberg-flyer.jpg)

To download this flyer as a Word document click here:

Jean Seberg Flyer (https://fightgangstalking.files.wordpress.com/2013/05/jean-seberg-flyer.docx)

Here is a third flyer which could stir things up:

The ACLU played no role in the exposure in 1971 of the FBI's illegal Cointelpro operations. Similarly – for reasons known only to its staff – the ACLU apparently never makes any public statements about the ongoing Cointelpro operations commonly referred to as "organized stalking" or "gang stalking."

The following flyer is an example of what the ACLU could send out
that would be helpful. Since I don't have the authority to issue public statements on behalf of that organization, I cannot officially say whether it would approve of this flyer.

You could try to contact the ACLU about it, although – in my experience – it is unlikely that you would receive a response to an inquiry about domestic counterintelligence stalking.

It would not surprise me therefore if some targets of organized stalking concluded that the only way to get the attention of the ACLU on this issue would be to anonymously mail/distribute/post flyers such as this one, and thereby generate some attention to the crime of organized stalking.

I have no expertise about the legal liability one might potentially face for distributing a document which bears the ACLU's logo and implies the organization's approval. To mitigate the risk of trouble, I included a disclaimer at the bottom.

Whatever risk might be associated with this, it is certainly less than the risk assumed by those who broke into an FBI office in 1971 and stole secret documents which exposed the Cointelpro operations being perpetrated at that time.

Click on image to enlarge

(https://fightgangstalking.files.wordpress.com/2013/05/aclu-flyer-image2.jpg)

To download this flyer as a Word document click here:

ACLU Flyer (https://fightgangstalking.files.wordpress.com/2013/05/aclu-flyer2.docx)

For any of the above flyers which you decide to distribute, I recommend bringing the file to a print shop or office supply store on a USB flash drive, and having them print a batch of flyers for you. That will be much cheaper than paying for the printer ink to print them yourself.

Consider distributing small leaflets also.

If you are distributing your flyers door-to-door rather than mailing them, you might be uncomfortable with full-size sheets of paper such as the one above. If so, consider using small leaflets instead.

Again, the most efficient way to do this is to have a print shop or office supply store print them. Here is a standard document you use.

Click on image to enlarge

(https://fightgangstalking.files.wordpress.com/2013/05/small-leaflet.jpg)

To download this leaflet as a Word document click here:

Small Leaflet (https://fightgangstalking.files.wordpress.com/2013/05/small-leaflet.docx)

Distribute handfuls of these generously and creatively. Perhaps you can incorporate the distribution into your walks/runs/bike rides. This tactic works especially well when it's windy.

Calibrate your distribution to correspond to the level of harassment you're experiencing. If the perps are only performing a few occasional small acts of harassment, you can distribute just a few of these small leaflets. If they are intensely harassing you on a constant basis, you can blanket the whole neighborhood.

Repeat as needed. 🙂

---

3. Business Cards

Business cards offer an excellent way to physically spread information around your neighborhood. They can be easily distributed to while on a walk or a bicycle ride. They are easy to toss onto a walkway or doorstep. They can be easily flicked over a gate or fence.

They can also be placed under vehicle windshield wipers – in residential neighborhoods or in parking lots.

Also, if you're being mobbed at a local business or at your workplace, you can start leaving the cards there in random places (on/in shelves, drawers, cabinets, chairs, counters, the floor, between the pages of books and magazines, next to the phone, under mouse-pads, etc.). Be creative.

You can purchase 500 business cards (printed in color on both sides) for about twenty bucks.

Here's a template you can use. Just click on the image to expand it, then right-click on the expanded image and save it as a .jpg file on your computer. Take the image on a thumb drive to a print shop (or email it to them) and have them create a business card with this printed on both sides.

(https://fightgangstalking.files.wordpress.com/2013/05/fgs-contact-card-rev-b.jpg)

If you cannot afford to have cards printed, take some pieces of heavy paper – such as file folders – and cut out a few business card-size pieces to make hand-written cards. Keep a few of them in your wallet. As long as they're legible, they will have the desired effect.

The next time you encounter a perp (the paid criminal informant variety or the volunteer useful idiot type), smile and take out a card. Hand it to him or her and say ***"Have you ever wondered exactly who you're working for?"*** If the perp refuses to accept the card, just say ***"Well, if you get curious, you can always find out"*** and toss the card on the ground.

The perp *will* be curious. After you walk away, he or she will probably return to pick up the card – if only to present it to the person who tells him or her what to do. Some of the perps – perhaps most – will take a look at this website and learn exactly what the whole business is about.

Law enforcement agencies and corporations which delegate some of their dirty work to security contractors and other lower-level minions do not want everyone to understand the whole process, so you will be throwing a wrench into the Stasi machine.

---

4. Window Signs & Bumper-Stickers

(https://fightgangstalking.files.wordpress.com/2013/05/fgs-banner-cropped.jpg)

Distributing flyers and business cards – as discussed above – are powerful tactics for calling attention to the criminals who are stalking you. However, the exposure they create is temporary. A sign posted inside a window of your residence can be left in place for a longer period.

Depending on the proximity of pedestrians and neighbors to your window (and the severity of the harassment), you might want to start with something small – such as one of the flyers or business cards. If needed, you can post a sign of whatever size needed for visibility.

This can create a real problem for the criminal perps who are stalking you. Anyone whose curiosity is piqued by such signs can visit this website and learn all about the nature of the illegal harassment.

A reader of this website who adopted this tactic sent this photograph of a banner which has been prominently displayed for the neighbors to consider.

Another excellent way to exploit this tactic is to place a sign inside the window of your vehicle – or to order a custom bumper sticker from any of the countless websites which perform that service.

---

5. Chalk Messages

(https://fightgangstalking.files.wordpress.com/2013/05/prang-chalk.jpg)
Scrawl chalk messages about gang stalking on the sidewalk near your residence.

Compared with paint graffiti, messages in chalk are far less likely to lead to any legal troubles. Be creative with the placement, size, colors, and wording of your messages. Be sure to include the term "gang stalking" or "gang stalkers."

If you know that the residence next-door is being used by perpetrators, you can write "Gang Stalking Perps" on the sidewalk in front of the residence, with an arrow pointing to the residence.

As with flyers and banners, the ideal message is "FightGangStalking.com" so you can convey exactly what is happening. At least a few of your neighbors will probably visit the website to find out what is going on.

Anyone participating in gang stalking will not want to attract attention to his crimes by making a big public issue about your sidewalk artwork. The same is true of the police. Therefore, sidewalk chalk messages are another opportunity for you to exploit the stalkers' fear of the "Streisand Effect."

If a neighbor who is not a gang stalker asks what you're doing, just tell him or her the truth and let the chips fall where they may. You're not the one engaged in the criminal felony of stalking.

You can purchase sidewalk chalk at toy stores and elsewhere, but I recommend that you instead use a more vibrant colored art-quality chalk which is less quickly washed away by rain – or by a perp with a garden hose.

In particular I recommend **"Prang Freart colored paper chalk"** (shown above) which you can purchase online or at certain art supplies shops. It's perfect for the job. Sidewalks are *extremely* abrasive, and most art-quality chalk – unlike this style – is sold in thin sticks which wear-down or break very quickly.

If you have reservations about using chalk which is difficult to clean-off of the pavement, another option is to start with water-soluble sidewalk chalk instead. If the harassment does not diminish, you can then try the chalk that is harder to ignore.

Here is an example of the water-soluble variety of sidewalk chalk which is widely available:

(https://fightgangstalking.files.wordpress.com/2013/05/crayola-chalk.jpg)

---

6. Self-Inking Stamps

(https://fightgangstalking.files.wordpress.com/2013/05/self-inking-stamp.jpg)

This excellent idea was submitted by a reader of this website.

Order a self-inking stamp with a message suited to exposing gang stalking. I would humbly suggest that you include the name of this website in the message – since it is both a statement and an instruction for where to go for more information.

Red ink and bold lettering would be appropriate.

Such stamps are cheap. They are also small and light-weight, so they are easy to carry with you – for example at your job if you are being mobbed by co-workers, or at a local business if you are being harassed there.

I'm guessing that gang stalking perps would not be pleased if the stamp mark began showing up on documents, phone books, invoices, letters, memos, booklets, restaurant menus, office football pool spreadsheets, etc.

You can also stamp your message on adhesive notes — which can be posted almost anywhere. Here are some photos which were emailed to me of such stamp marks showing up on a community bulletin board and a gas pump.

(https://fightgangstalking.files.wordpress.com/2013/05/stamp-on-bulletin-board.jpg)

(https://fightgangstalking.files.wordpress.com/2013/05/stamp-on-gas-pump.jpg)

Using currency to spread news about government corruption

I try to avoid recommending tactics which might technically violate any laws – even when they involve virtually zero chance of leading to any legal trouble. I do feel free however, to share information given to me by readers of my website about tactics they have chosen to use.

Apparently, ink-stamps such as the one shown above are being used by some victims of organized stalking to mark dollar bills (on both sides). U.S. currency seems like a symbolically perfect vehicle for transmitting a warning about the deep rot in the U.S. government. Also, unlike an adhesive note, a dollar bill is unlikely to be thrown away; any message it contains will be seen by numerous people over a long period of time.

Although I suspect that the U.S. Treasury Department might not view this tactic as being legally kosher, I can certainly understand why some victims of America's Stasi are exploiting it. Others are using this tactic too. The co-founder of Ben & Jerry's ice cream used this method to bring attention to the role of corporate money in American politics, as reported here. (http://readersupportednews.org/news-section2/440-occupy/11771-ben-a-jerrys-co-founder-occupy-dollar-bills)

(https://fightgangstalking.files.wordpress.com/2013/05/stamp-messages-on-currency.jpg)

In my view, the most effective ink-stamp message would include more than just the name of the website. **A stamp such as this would be ideal:**

Expose COINTELPRO Crimes
Google "Fight Gang Stalking"

With an ink stamp, you could easily mark both sides of a whole batch of bills very quickly, and the marks would all be legible. If you can't afford the $20 to $25 that a stamp would cost though, you could write the message by hand instead:

(https://fightgangstalking.files.wordpress.com/2013/05/dollar-with-message.jpg)

---

7. Banners

(https://fightgangstalking.files.wordpress.com/2013/05/overpass-banner.jpg)
Hanging a banner is a slightly bolder guerrilla tactic, and one which is harder to do without mutiple people, but you might want to consider it.

The ideal location would be a freeway overpass during rush-hour – assuming you can make certain there is zero risk of the banner falling onto the roadway, but even a small banner in a less exposed location could get some helpful attention.

Again, the ideal message would probably be "FightGangStalking.com" since you can't pack much information into a sign.

If you do hang a banner somewhere, try to get a photo of it and email it to me so I can post it on this website.

Here is an example of a website with tips about banners. (http://ioncoalition.net/sign-making-tips/)This particular site happens to have an anti-Obama orientation, but I presume the logistics of banners are a non-partisan matter. I considered including advice from the animal rights group PeTA as well, since they hold a lot of protests. But it occurred to me that if you can talk famous actresses and models into posing naked for you, I'm guessing you don't need any advice from me about anything.

---

8. Calling the police

(https://fightgangstalking.files.wordpress.com/2013/05/call-the-cops.jpg)

If you have read the "Tactics" section of the "What is Gang Stalking?" page of this website – or if you have experienced organized stalking harassment first-hand – you might be familiar with the psyops tactic called "gas-lighting." That is when stalkers enter the victim's residence while the victim is away and move or hide an object (or several objects) – or perhaps take something which will be noticed but which has minimal value.

Typically the victim of such incidents will either wonder whether the object has simply been misplaced, or will realize what has happened but not report it to the police because of (a) concern that local law enforcement officials are complicit in the stalking, or (b) because of concern that it will sound ridiculous to make a claim that someone entered the residence and stole something of minimal value – while leaving other items untouched.

The tactic is diabolical – which is why it has been used in counterintelligence operations by agencies in multiple countries for decades. The intent is partly to cause the victim to question his or her own memory, but more seriously, to send the message that one's residence offers no shelter.

Don't play the stalkers' game by their rules; play by your own rules. They assume you will not call the police, so you should call the police.

The very fact that organized stalking almost always involves harassment tactics whose objectively-visible evidence is just below the threshold normally involved in reported crimes proves that the stalkers do not want to have police reports generated.

Of course, calling the police won't result in anyone being arrested and convicted of residential burglary, but it will force the police department to answer your call (which will be recorded) and to dispatch officers to take a report (which will be documented). Their visit will also likely attract the attention of your neighbors.

Note that this counter-measure would also be appropriate for other psyops tactics which are calculated to remain below the radar of official police reports – such as veiled threats and minor acts of vandalism.

Before calling the emergency dispatcher, you should seriously consider the option of mentioning that you are not sure whether the intruder is still in your residence – because the intruder could still be present theoretically. That might create the need for a more significant and urgent response. If you have a dog though, you will need to consider how to keep it safe, as American cops seem to have a penchant for shooting them. (http://reason.com/blog/2014/06/27/cops-shot-at-retreating-arthritic-dog-to)

When the officers arrive, ask them what they know about gang stalking; they will be forced to lie to you and feign ignorance about the subject. The discussion might at least be awkward for the officers – especially if they are not morally corrupt. They will very likely see from your demeanor that you are apparently sincere.

Ideally, you should record their visit with audio and/or video. You should also insist that your concerns about organized stalking be included in the report.

The more time and effort you invest in pursuing the matter the better. Consider calling and/or writing to the police department requesting a copy of the report – or at least the report number. State laws regarding freedom of information requests where you reside very likely will make it possible for you to request information about the incident.

Also consider calling and/or writing to other city officials indicating that a disturbing crime has occurred involving a residential break-in. Consider reporting the incident(s) to your local newspaper also.

You might also consider mailing flyers to all your neighbors about the incident.

The more such actions you take, the more effective this tactic will be. You need to give the perps a reason to refrain from such criminal behavior in the future.

None of this will please the local police department – regardless of their level of involvement or their awareness of organized stalking activity by federal agencies and corporate security contractors. Because of that, your stalkers might consider it more trouble than it is worth to repeat their stunt.

You might be concerned that local authorities will object to what seems like a "frivolous" police report, but remember: they will not want to bring about the Streisand Effect by aggressively trying to discourage your reporting of the incidents. Your insistence on making an issue of what is happening can create a real problem for local authorities.

---

9. Interacting with Police Officers

(https://fightgangstalking.files.wordpress.com/2013/05/respect-my-authority.jpg)
Direct interactions with targeted individuals are rarely initiated by law enforcement officers – especially officials who identify themselves as such. Out-sourced overt stalking by agencies and corporations is much more common. Nevertheless, you should be aware of your legal rights in case such encounters occur.

Here is some advice about what to do if law enforcement agents (local police, FBI, etc.) want to talk to you – or to your friends, roommates, co-workers, relatives, or acquaintances. You should read these instructions and memorize the few main points.

Advice from the ACLU (American Civil Liberties Union)

Know Your Rights (https://www.aclu.org/drug-law-reform-immigrants-rights-racial-justice/know-your-rights-what-do-if-you)

Advice from the CDLC (Civil Liberties Defense Center)

FBI-Script (https://fightgangstalking.files.wordpress.com/2013/05/fbi-script.pdf)

Here is the nutshell version of what to do if a cop or agent wants to talk to you:

"Make no statement to the police under any circumstances."

– Robert Jackson, U.S. Supreme Court Justice
Watts v. Indiana, 338 U.S. 49 (1949)

(https://fightgangstalking.files.wordpress.com/2013/05/blue-line3.jpg)

E. Exposing the Perps Nationally

(https://fightgangstalking.files.wordpress.com/2013/05/national-exposure.jpg)
The first prong of the strategy to undermine America's Stasi is to expose organized stalking crimes locally; the second prong is to expose what is happening on a national level.

Be aware that these outreach tactics can have a powerful effect even if they do not generate immediate replies. The fact that a particular letter, email, phone call, or online comment does not necessarily produce a direct visible reaction should not discourage you. The impact is cumulative. Awareness and discussion of gang stalking will spread a little bit every time you use any of these tactics. Eventually, the Stasi rodent industry will mostly collapse from exposure.

1. Letters to Congress

(https://fightgangstalking.files.wordpress.com/2013/05/letters.gif)

General Strategy

Members of Congress rarely act upon an issue simply out of a desire to stop an injustice. Instead, they mostly take actions in response to pressure. Since victims of organized stalking are a non-powerful minority of the electorate, their rights are not likely to be viewed as important even if stalking crimes are brought to the attention of legislators. Consequently, this tactic is only one element of a larger strategy.

At the end of this webpage, I address an even more vital component of the exposure process – namely, letters to the news media. Ultimately, pressure on Congress to investigate and end organized stalking will mostly come from a need to respond to increasingly frequent news reports on the topic.

Still, sending letters to your representatives in Congress calling for an investigation into domestic counterintelligence crimes is a smart thing to do, and it requires very little time and effort. You should send your letter (or email) to the member of the House of Representatives who represents your congressional district, and to both of your state's senators.

Contact Information

The official webpage of the House of Representatives (http://www.house.gov/)will show you who your representative is if you type in your zip code. Then just click on the envelope icon next to the photo of your representative to get to his or her contact page.

The official webpage of the Senate (https://www.senate.gov/)provides the contact information for your senators. You can look them up by your state or by your senators' names.

A Standard Letter You Can Use

The easiest way to exploit the tactic of sending letters is to use the letter I have drafted (the link is at the end of this section) – which can be sent exactly as it is to any government official or member of the news media. You only need to add the name and address of the recipient, your name and address, and the date.

Tips for Writing Your Own Letter

If you have the writing skills and free time to compose and proofread a letter which will be taken seriously, then create a persuasive letter calling for an investigation into the crime of organized stalking.

Postal letters are widely believed to be more effective than emails, and I share that view. Their physical nature conveys more seriousness than that of an email. That said, emails are obviously more convenient for the sender – and they have the advantage of being easier to respond to and to forward for the recipient.

You should use the term "gang stalking" sparingly. Most people are unfamiliar with the term and are also likely to mistakenly assume it has something to do with street gangs. In addition, those few people who have seen the term previously – or who bother to perform a cursory search online – are likely to have their perception distorted by the vast amount of disinformation, and are likely to just dismiss your concerns as paranoia. The term "organized stalking" is slightly better, but better still are phrases such as "stalking crimes involving counterintelligence tactics."

Emphasize mainstream published news reports rather than your personal experiences. You might want to mention that you are a victim of organized stalking, but be aware that for some readers it will undermine your credibility. Some recipients of your letter will assume that you are either paranoid or that you should be contacting the police department instead.

Consider writing your letter in the form of a question rather than an assertion. Although you are in a position to be certain of the reality of gang stalking, the person to whom you are writing does not have such first-hand experience, and cannot know whether your claims are credible. So instead of saying "this is happening and you should look into it," it might be more productive to ask whether the person you are writing to has any knowledge of the media reports about what appear to be domestic counterintelligence operations, and suggesting that an investigation is in order.

If you choose to write your own letters, you might want to visit this website (http://advocacyguru.com/resources/faqs/) which has helpful advice about how to contact a member of Congress.

Do not be discouraged if you do not receive replies. At a minimum, your letters will be reviewed by office staff members and some of the letters will generate discussion. Also, letters received by members of Congress will at least be recorded, as required by law.

Contacting Other Members of Congress

Generally, members of the House only concern themselves with letters from constituents who reside within their district. Similarly, senators normally are not interested in letters from residents of other states. If you still want to send additional letters to Congress – it can't hurt – you should probably direct them to those legislators who have a reputation for being concerned about civil rights.

As I write this, some of the Congress members known to champion civil rights issues include the following people: Senator Ron Wyden (D-Oregon), Senator Rand Paul (R-Kentucky), Representative Justin Amash (R-Michigan), and Representative Alan Grayson (D-Florida).

Here are the contact pages of the websites of those Congress members:

http://www.wyden.senate.gov/contact (http://www.wyden.senate.gov/contact)

http://www.paul.senate.gov/?p=contact (http://www.paul.senate.gov/?p=contact)

https://amash.house.gov/contact-me/email-me (https://amash.house.gov/contact-me/email-me)

https://grayson.house.gov/contact/email-me (https://grayson.house.gov/contact/email-me)

Secrecy Oaths

Because of their privileged access to classified information, members of the House and Senate intelligence committees – such as Senator Wyden – might already be well aware that an unethical and unconstitutional form of domestic counterintelligence operations is being perpetrated.

Members of the intelligence committees have presumably never been officially told about all of the extremely illegal activities involved in organized stalking as it is actually practiced, but they might be aware that some extensive network of "informants" is being managed by counterintelligence specialists.

Unfortunately, the secrecy oaths taken by members of those committees legally prohibit them from disclosing – even to fellow Congress members – the details of such programs. That oath applies even if the committee members believe a program is unconstitutional.

Although it would be admirable for those Congress members to speak out against such crimes despite the potential legal and career consequences, such acts of self-sacrifice are exceedingly rare among politicians. Nevertheless, letters about gang stalking could at least generate some discussion among committee members – and among their staffers.

Contacting State & Local Officials

Another smart move would be to send your letter to your representatives in your state's legislature – and other state officials, such as your state's attorney general and governor.

A Standard Letter You can Send

Here is the letter I drafted that can be sent to any official (or reporter).

As I mentioned, the ideal format is to mail a hard copy of the letter. If you choose to send it via email, I recommend that you copy and paste the letter into the body of your email rather than sending the letter as an attachment because many people are wary of opening email attachments.

Click here to download the letter as a Word document:

U.S. Domestic Counterintelligence (https://fightgangstalking.files.wordpress.com/2013/05/u-s-domestic-counterintelligence1.docx)

---

2. Online Petitions

(https://fightgangstalking.files.wordpress.com/2013/05/scroll-and-pen.jpg)

I include this tactic mainly for the sake of being complete. Although an online petition can be created easily and with no expense, it is very unlikely to gain the attention of anyone who can help expose the FBI's counterintelligence subversion program (gang stalking).

If you are trying to communicate to members of Congress, your best bet is to send letters (especially actual postal letters rather than emails) as discussed above.

I don't wish to discourage anyone from trying to create a serious credible petition, but you should be aware of the limitations and challenges.

First, do not confuse online petitions with the professionally-organized petitions associated with state ballot propositions. An online petition has no legal significance. It is merely something which – at best – can be cited as evidence of popular support.

Another problem is that people who electronically "sign" petitions must include their name and address. Many – perhaps most – victims of gang stalking will be reluctant to do that for various obvious reasons.

In addition, this avenue has already been corrupted by the FBI's minions – who have posted a number of fake petitions as disinformation (for an example, see the one on the FFCHS page of this website). Similarly, even legitimate petitions seeking to expose gang stalking can be easily discredited by the FBI simply by having sock puppets post idiotic comments under them and by adding false "signatures" accompanied by statements intended to convey paranoia and stupidity.

I have seen several online petitions directed to state attorneys general and to members of Congress to investigate gang stalking, but they were not credible. As evidence of the crimes, the petitions cited information sources such as blogs or disinformation websites or fake (non-edited) online newspapers, such as examiner.com, etc.

As with many websites about gang stalking, it is difficult to determine whether the petitions were even created by targeted individuals. I suspect they were deliberate disinformation.

If you wish to pursue this tactic despite the above considerations, here are a few of the websites which provide platforms:

www.change.org (http://www.change.org/)

www.petition2congress.com (http://www.petition2congress.com/)

http://www.credomobilize.com/ (http://www.credomobilize.com/)

If you do create a petition – or locate a credible existing one, your petition statement should cite some of the published mainstream news reports listed on the *What is "Gang Stalking?"* page of this website, and you should promote your petition via social media (Facebook, Twitter, email, blogs, etc.).

---

3. Calls to Radio Programs

(https://fightgangstalking.files.wordpress.com/2013/05/radio.jpg)
Call a radio talk show which is covering an issue that is even remotely related to gang stalking (government surveillance, law enforcement, etc.), and mention that many news reports suggest that there seems to be a current version of Cointelpro going on which borrows heavily from the tactics of communist East Germany's Stasi.

Cite some of the news reports listed in the *What is "Gang Stalking?"* page of this website. Ask the host or guest if he or she agrees that it might be a good idea for the U.S. Senate to hold another version of the Church Committee investigations – as was done in the 1970s.

You don't need to be able to lay out the whole case about organized stalking – although if you have read the material posted on this website you will know far more about police state issues than do most people.

One option is to simply mention the list of publications which have called for another Church Committee investiagion – which you can find in the March 13, 2014 post of the Cointelpro News page of this website.

A large audience could hear about gang stalking for the first time and that would be a great achievement. It would be a lot easier than trying to persuade some program manager to schedule a show on the subject.

A reader of this website used this tactic in July 2013. During a radio talk show segment about how whistle-blowers are treated in the workplace, she called to inquire about the issue of "mobbing" – the organized harassment of an individual by bosses and co-workers.

She told me that she had been harassed in her workplace as part of her gang stalking and when she reported the harassment, the managers initially tried to dismiss the whole matter. When she pursued the issue, they did take it seriously, but then she was retaliated against and eventually fired.

The show's guests – an employment attorney and a psychologist – were both familiar with mobbing, but many of the program's listeners were no doubt unfamiliar with the phenomenon, so it helped to spread awareness of it.

A recording of the program is posted here. (http://www.newhaven.edu/news-events/UNH-in-the-media/2013-2014/591194/) Click on "Download Audio." The relevant segment is from 40:33 to 48:25

---

4. Freedom of Information Act (FOIA) Requests

(https://fightgangstalking.files.wordpress.com/2013/05/foia.jpg)

Anyone targeted by organized stalking should consider trying to exploit his or her rights under the Freedom of Information Act (FOIA) to obtain information about what is happening.

The U.S. government's official website about FOIA (http://www.foia.gov/about.html)describes the act this way:

"Enacted on July 4, 1966, and taking effect one year later, the Freedom of Information Act (FOIA) provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions."

FOIA requests can be used to (possibly) find information about your personal situation – for example, whether you are under investigation or on a watch list. It can also (possibly) be used to find information about organized stalking generally.

Fortunately the act is intended to enable average citizens – not just lawyers and investigative journalists – to obtain information about the government's activities. In addition to the official FOIA website above, many sites offer tips about filing FOIA requests. Here are a few examples:

ACLU advice on FOIA
(http://www.skepticfiles.org/aclu/foia.htm)

Citizen's guide from Congress on how to make FOIA requests
(http://www.fas.org/sgp/foia/citizen-2012.pdf)

Exploiting privacy waivers when making FOIA requests (http://www.motherjones.com/politics/2013/11/foia-ryan-shapiro-fbi-files-lawsuit)

Freedom of Information requests for ***state*** *records* (http://www.nfoic.org/state-sample-foia-request-letters)
(http://www.nfoic.org/state-sample-foia-request-letters)

Websites which assist you in submitting FOIA requests:

An example of a site dedicated to helping people submit FOIA requests is ***Muckrock.*** (https://www.muckrock.com/) As of March 2014, Muckrock allows its users to submit 5 FOIA requests for just $20. The website's staff includes people with journalism and technology backgrounds.

Here is the website's description of its purpose:

Filing Freedom of Information Requests doesn't need to be difficult. At MuckRock, we are dedicated to wading through the muck so you don't. What does this mean for you? Less time spent mitigating complex bureaucratic processes so that you can focus on analyzing and reporting on the issues that matter most to you and your organization or business.

As the only public records request service of its kind in the United States, MuckRock serves journalists, researchers, activists and historians, with a track record of over 2,000 requests. Simply log-in to your account and submit your FOI request via our simple web-interface.

MuckRock acts as a request proxy, e-mailing, faxing or even snail mailing the request on your behalf. Documents are sent to our offices to be prepared by our team of experts for your convenience. We can even assist with analyzing your data. Our intuitive system ensures that your documents are for your eyes only until you're ready to publish.

Here are some examples (https://www.muckrock.com/accounts/profile/Cdweissenberg/) of gang stalking-related document requests filed by one person.

Here is the MuckRock site page about *requesting your FBI file.* (https://www.muckrock.com/news/archives/2013/jun/21/foia-how-getting-your-own-fbi-file/)

General tips:

To exploit the FOIA to obtain information about gang stalking, you should give some thought to creative angles of attack. The exact wording of your FOIA request can make a huge difference. Requests are frequently denied for being too vague, for example.

Also consider the advantage of requesting information in an oblique way. Instead of seeking only information about "gang stalking," you should consider looking for information about "surveillance role players" and "InfraGard" and other official key words.

Another productive angle might be to seek information about inquiries made by gang stalking victims – of which there must be many. The Department of Justice and Congress have no doubt received such questions.

A caveat about making FOIA requests

While I encourage the use of FOIA requests to pry information from the U.S. government, I would advise you to be realistic about the prospects. To a great extent, the federal agencies which have the most scandals to hide have undermined the purpose of FOIA by adopting a policy of routinely denying legitimate information requests. Such a denial forces the individual making the request to file a lawsuit, and many people lack the time and money needed for such lawsuits. This May 2014 article by *Techdirt* (https://www.techdirt.com/articles/20140429/11334527064/governments-antipathy-towards-transparency-has-made-foia-lawsuits-default-process.shtml) explains how the feds use this strategy to fight against transparency.

"These agencies know that not everyone has the time or money to battle for the release of documents, so their exposure is limited should they choose not to comply."

Naturally, you should not expect help in this area from the U.S. Department of Justice (DOJ), since they are one of the intelligence agencies which is apparently complicit in counterintelligence stalking. The *Techdirt* article also notes that the DOJ naturally favors government secrecy over transparency and public accountability.

"The DOJ likely has no problem with the DHS, CBP and others blowing off FOIA requests until the judicial system orders them to turn over the requested info."

---

5. Posting Comments Online

(https://fightgangstalking.files.wordpress.com/2013/05/cat-typing.jpg)

One of the quickest and easiest ways to spread awareness about illegal spying and vigilantism by corrupt cops is by posting comments and links online. Try to direct attention to this website.

---

6. Letters & Emails to Journalists & Non-Profit Groups

(https://fightgangstalking.files.wordpress.com/2013/05/typewriter.jpg)

Send letters to news outlets, non-profit organizations, friends, and relatives. You can use the exact same standard letter mentioned above for contacting members of Congress.

Contacting News Agencies

Contact local and national newspapers, magazines, TV and radio programs, and websites – the more the better – and suggest that they do a story on gang stalking.

Don't ask them to do the story as a public service; pitch it as something which would be interesting for their readers/viewers/listeners. Mention that there is a lot of Internet discussion about the subject (you can mention, for example, a few of the main gang stalking websites, such as this one and the sites in the "Recommended Websites" page of this blog).

Instead of addressing your letters generically to an organization (such as a news agency), it is far better to look-up the name of a particular person at the organization if possible and address it to him or her specifically.

Contacting the ACLU

Apparently the ACLU does not respond to inquiries about gang stalking – or discuss the subject on its website. You might still want to send a letter or email to them just to remind them that we know that they know what is happening.

Beyond a single letter, I would not waste much time trying to contact their national office. A better approach is to do a Google search for the local ACLU chapter closest to you, and attend one of their meetings in person. Ask them whether they are familiar with gang stalking and if they will try to help gain the attention of the national ACLU office on the issue.

Remember though: the ACLU did not expose the first version of Cointelpro, and they have shown no interest in exposing its current version. By all indications, the ACLU's national office plans to wait until it is safe before they wade into this issue.

Contacting Other Organizations

Cast a very wide net when gathering addresses to which you can send your letters. Include schools (teachers and administrators), churches, businesses, colleges (professors and administrators), private organizations, amusement parks, Civil War reenactment groups, whatever.

Of course, many of those people will have no direct connection or familiarity with issues involving illegal law enforcement tactics – but that's exactly the point. Gang stalkers want to keep their secrets within their own gang. You can make that impossible.

Here again is the standard letter which can be used for contacting reporters, government officials, non-profit groups, and others.

Click here to download the letter as a Word document:

U.S. Domestic Counterintelligence (https://fightgangstalking.files.wordpress.com/2013/05/u-s-domestic-counterintelligence1.docx)

Go disrupt the game of the counterintelligence pigs!

(https://fightgangstalking.files.wordpress.com/2013/05/angry-birds-v-perps1.jpg)

A final thought…

Fighting the U.S. government's Stasi brigade of corrupt cops, snitches, bullies, liars, parasitic security contractors, sociopaths, traitors, and useful-idiot vigilantes is a fight worth having – even if you are unsure of the prospects for a quick victory. Journalist and political activist Chris Hedges gave a speech in Santa Monica, California on October 13, 2013 in which he addressed that point:

"I do not fight fascists because I will win.
I fight fascists because they are fascists."

If you can help expose illegal spying and harassment of Americans by intelligence agencies, law enforcement agencies, and private security contractors, please do so. America needs more patriots like Daniel Ellsberg, Edward Snowden, Jeremy Hammond, Barrett Brown, Russell Tice, William Binney, Ray McGovern, Thomas Drake, Frank Serpico, Thomas Tamm, Hugh Thompson, Jr., William C. Davidon, John Raines, Bonnie Raines, Keith Forsyth, Judi Feingold, and Bob Williamson.

(https://fightgangstalking.files.wordpress.com/2013/05/anti-nazi-image.jpg)

(https://fightgangstalking.files.wordpress.com/2013/05/glider.png)

FightGangStalking.com

STRATEGIC STUDIES QUARTERLY

Commanding the Trend: Social Media as Information Warfare

Lt Col Jarred Prier, USAF

Abstract

This article demonstrates how social media is a tool for modern information-age warfare. It builds on analysis of three distinct topics: social networking, propaganda, and news and information sharing. Two case studies are used to show how state and nonstate actors use social media to employ time-tested propaganda techniques to yield far-reaching results. The spread of the propaganda message is accomplished by tapping into an existing narrative, then amplifying that message with a network of automatic "bot" accounts to force the social media platform algorithm to recognize that message as a trending topic. The first case study analyzes Islamic State (IS) as a nonstate actor, while the second case observes Russia as a state actor, with each providing evidence of successful influence operations using social media. Coercion and persuasion will continue to be decisive factors in information warfare as more countries attempt to build influence operations on social media.

✳ ✳ ✳ ✳ ✳

For years, analysts in the defense and intelligence communities have warned lawmakers and the American public of the risks of a cyber Pearl Harbor. The fear of a widespread cyber-based attack loomed over the country following intrusions against Yahoo! email accounts in 2012, Sony Studios in 2014, and even the United States government Office of Personnel Management (OPM) in 2015. The average American likely did not understand exactly how, or for what purposes, US adversaries

Lt Col Jarred Prier, USAF, currently serves as director of operations for the 20th Bomb Squadron. He completed a USAF fellowship at the Walsh School of Foreign Service at Georgetown University and earned a master's degree from the School of Advanced Air and Space Studies at Air University, Maxwell Air Force Base, Alabama. Prier also holds a master of science degree in international relations from Troy University, Alabama. This article evolved from his thesis.

were operating within the cyber domain, but the implications of future attacks were not difficult to imagine. Enemies of the United States could target vulnerable power grids, stock markets, train switches, academic institutions, banks, and communications systems in the opening salvos of this new type of warfare.[1]

In contrast to more traditional forms of cyberattack, cyber operations today target people within a society, influencing their beliefs as well as behaviors, and diminishing trust in the government. US adversaries now seek to control and exploit the trend mechanism on social media to harm US interests, discredit public and private institutions, and sow domestic strife. "Commanding the trend" represents a relatively novel and increasingly dangerous means of persuasion within social media. Thus, instead of attacking the military or economic infrastructure, state and nonstate actors outside the United States can access regular streams of online information via social media to influence networked groups within the United States. This article analyzes how two US adversaries hijacked social media using four factors associated with command of the trend. First it provides a basis for commanding the trend in social media by analyzing social media as a tool for obtaining and spreading information. It then looks more specifically at how US adversaries use social media to command the trend and target US citizens with malicious propaganda. Next, the two most prominent, recent case studies provide evidence of how nonstate and state actors use social media to counter the United States. The first case study covers IS from 2014 to 2016 by examining the group's use of social media for recruiting, spreading propaganda, and proliferating terror threats. The second case describes the pattern of Russian hacking, espionage, disinformation, and manipulation of social media with a particular focus on the United States presidential election of 2016. Evidence for this second case study comes from nearly two years of research on Twitter accounts believed to be part of a Russian information warfare network. The article concludes with implications and predictions of how social media will continue to develop, what can be expected in the future, and how the United States can respond to the growing threat of adversaries commanding the trend.

Commanding the Trend in Social Media

The adaptation of social media as a tool of modern warfare should not be surprising. Internet technology evolved to meet the needs of

information-age warfare around 2006 with the dawn of Web 2.0, which allowed internet users to create content instead of just consuming online material. Instead, the individual could decide what was important and only read what was important, on demand. Not only could users select what news they want to see, but they could also use the medium to create news based on their opinions.[2] The social nature of humans ultimately led to virtual networking. As such, traditional forms of media were bound to give way to a more tailorable form of communication. US adversaries were quick to find ways to exploit the openness of the internet, eventually developing techniques to employ social media networks as a tool to spread propaganda. Social media creates a point of injection for propaganda and has become the nexus of information operations and cyber warfare. To understand this we must examine the important concept of the social media trend and look briefly into the fundamentals of propaganda. Also important is the spread of news on social media, specifically, the spread of "fake news" and how propaganda penetrates mainstream media outlets.

Trending Social Media

Social media sites like Twitter and Facebook employ an algorithm to analyze words, phrases, or hashtags to create a list of topics sorted in order of popularity. This "trend list" is a quick way to review the most discussed topics at a given time. According to a 2011 study on social media, a trending topic "will capture the attention of a large audience for a short time" and thus "contributes to agenda setting mechanisms."[3] Using existing online networks in conjunction with automatic "bot" accounts, foreign agents can insert propaganda into a social media platform, create a trend, and rapidly disseminate a message faster and cheaper than through any other medium. Social media facilitates the spread of a narrative outside a particular social cluster of true believers by commanding the trend. It hinges on four factors: (1) a message that fits an existing, even if obscure, narrative; (2) a group of true believers predisposed to the message; (3) a relatively small team of agents or cyber warriors; and (4) a network of automated "bot" accounts.

The existing narrative and the true believers who subscribe to it are endogenous, so any propaganda must fit that narrative to penetrate the network of true believers. Usually, the cyber team is responsible for crafting the specific message for dissemination. The cyber team then generates

videos, memes, or fake news, often in collusion with the true believers. To achieve the effective spread of propaganda, the true believers, the cyber team, and the bot network combine efforts to take command of the trend. Thus, an adversary in the information age can influence the population using a variety of propaganda techniques, primarily through social media combined with online news sources and traditional forms of media.

A trending topic transcends networks and becomes the mechanism for the spread of information across social clusters. Here the focus is primarily on Twitter, a "microblogging" site where each post is limited to 140 characters.[4] Facebook also has a trends list, but it is less visible than the Twitter trends list, and the two applications serve different purposes. Facebook maintains a function of bringing friends and families together. On Facebook, your connections are typically more intimate connections than you would expect on Twitter, which focuses less on bringing people together and more on bringing ideas together. As a microblog, Twitter's core notion is to share your thoughts and feelings about the world around you with a group of people who share similar interests. The individuals who follow each other may not be friends but could be a team of like-minded academics, journalists, sports fans, or politicos. When a person tweets, that tweet can be viewed by anyone who follows that person, or anyone who searches for that topic using Twitter's search tool. Additionally, anyone can "retweet" someone else's tweet, which broadcasts the original to a new audience. Twitter makes real-time idea and event sharing possible on a global scale.[5] Another method for quick referencing on Twitter is using a "hashtag." The tweet would then be visible to anyone who clicked on the link along with all of the other tweets using the same hashtag.

A trend can spread a message to a wide group outside of a person's typical social network. Moreover, malicious actors can use trends to spread a message using multiple forms of media on multiple platforms, with the ultimate goal of garnering coverage in the mainstream media. Command of the trend is a powerful method of spreading information whereby, according to an article in the *Guardian*, "you can take an existing trending topic, such as fake news, and then weaponise it. You can turn it against the very media that uncovered it."[6]

Because Twitter is an idea-sharing platform, it is very popular for rapidly spreading information, especially among journalists and academics;

however, malicious users have also taken to Twitter for the same benefits in recent years. At one time, groups like al-Qaeda preferred creating websites, but now, "Twitter has emerged as the internet application most preferred by terrorists, even more popular than self-designed websites or Facebook."[7] Twitter makes it easy to spread a message to both supporters and foes outside of a particular network. Groups trying to disseminate a message as widely as possible can rely on the trend function to reach across multiple networks.

Three methods help control what is trending on social media: trend distribution, trend hijacking, and trend creation. The first method is relatively easy and requires the least amount of resources. Trend distribution is simply applying a message to every trending topic. For example, someone could tweet a picture of the president with a message in the form of a meme—a stylistic device that applies culturally relevant humor to a photo or video—along with the unrelated hashtag #SuperBowl. Anyone who clicks on that trend list expecting to see something about football will see that meme of the president. Trend hijacking requires more resources in the form of either more followers spreading the message or a network of "bots" (autonomous programs that can interact with computer systems or users) designed to spread the message automatically. Of the three methods to gain command of the trend, trend creation requires the most effort. It necessitates either money to promote a trend or knowledge of the social media environment around the topic, and most likely, a network of several automatic bot accounts.

Bot accounts are non-human accounts that automatically tweet and retweet based on a set of programmed rules. In 2014, Twitter estimated that only 5 percent of accounts were bots; that number has grown along with the total users and now tops 15 percent.[8] Some of the accounts are "news bots," which just retweet the trending topics. Some of the accounts are for advertising purposes, which try to dominate conversations to generate revenue through clicks on links. Some bots are trolls, which, like a human version of an online troll, tweet to disrupt the civil conversation.

For malicious actors seeking to influence a population through trends on social media, the best way to establish trends is to build a network of bot accounts programmed to tweet at various intervals, respond to certain words, or retweet when directed by a master account. Figure 1 illustrates the basics of a bot network. The top of the chain is a small

core group. That team is composed of human-controlled accounts with a large number of followers. The accounts are typically adversary cyber warriors or true believers with a large following. Under the core group is the bot network. Bots tend to follow each other and the core group. Below the bot network is a group consisting of the true believers without a large following. These human-controlled accounts are a part of the network, but they appear to be outsiders because of the weaker links between the accounts. The bottom group lacks a large following, but they do follow the core group, sometimes follow bot accounts, and seldom follow each other.

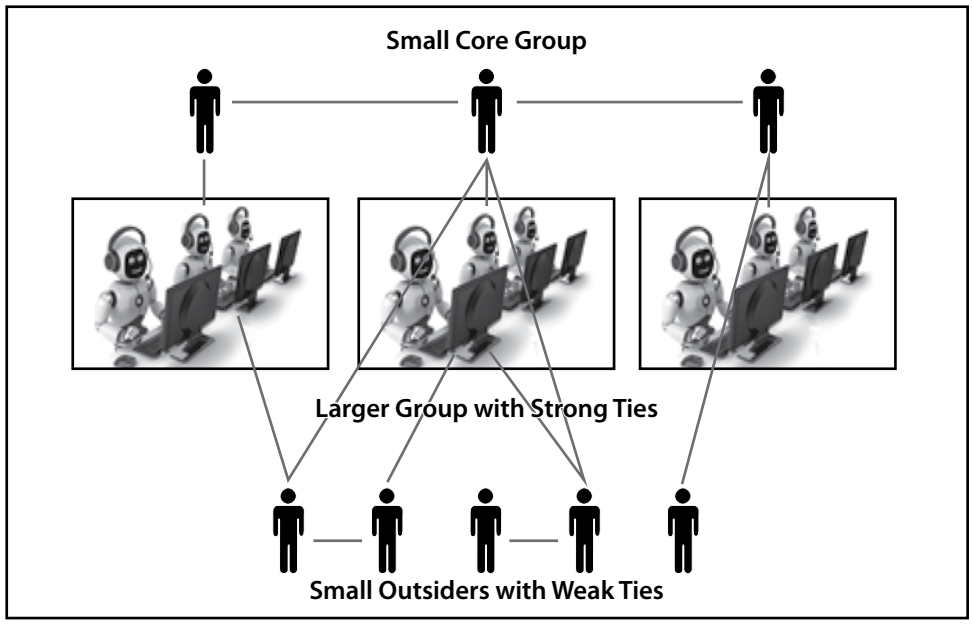


Figure 1. Illustration of a bot network

Enough bots working together can quickly start a trend or take over a trend, but bot accounts themselves can only bridge the structural hole between networks, not completely change a narrative. To change a narrative, to conduct an effective influence operation, requires a group to combine a well-coordinated bot campaign with essential elements of propaganda.

Propaganda Primer

Messaging designed to influence behavior has been around for centuries but became easier as methods of mass communication enabled wider dissemination of propaganda. Observing the rise of mass media and its presence in daily life, French philosopher Jacques Ellul noted the simplicity of propaganda in 1965. According to Ellul, "Propaganda ceases where simple dialogue begins."[9] That said, it is worth noting Eric Hoffer's comments that "propaganda on its own cannot force its way into unwilling minds, neither can it inculcate something wholly new."[10] For propaganda to function, it needs a previously existing narrative to build upon, as well as a network of true believers who already buy into the underlying theme. Social media helps the propagandist spread the message through an established network. A person is inclined to believe information on social media because the people he chooses to follow share things that fit his existing beliefs. That person, in turn, is likely to share the information with others in his network, to others who are like-minded, and those predisposed to the message. With enough shares, a particular social network accepts the propaganda storyline as fact. But up to this point, the effects are relatively localized. The most effective propaganda campaigns are not confined just to those predisposed to the message. Essentially, propaganda permeates everyday experiences, and the individual targeted with a massive media blitz will never fully understand that the ideas he has are not entirely his own. A modern example of this phenomenon was observable during the Arab Spring as propaganda spread on Facebook "helped middle-class Egyptians understand that they were not alone in their frustration."[11] In short, propaganda is simpler to grasp if everyone around a person seems to share the same emotions on a particular subject. Even a general discussion among the crowd can provide the illusion that propaganda is information.[12] In other words, propaganda creates heuristics, which is a way the mind simplifies problem solving by relying on quickly accessible data. The availability heuristic weighs the amount and frequency of information received, as well as recentness of the information, as more informative than the source or accuracy of the information.[13] Essentially, the mind creates a shortcut based on the most—or most recent—information available, simply because it can be remembered easily. Often, the availability heuristic manifests itself in information received through media coverage. The availability heuristic is important to understanding individual opinion formation and how propaganda can exploit the shortcuts our minds make to form opinions. The lines in figure 2 show formation

of opinions temporally, with bold arrows influencing a final opinion more than light arrows. The circled containers indicate a penetration point for propaganda exploitation. As previously described, mass media enables rapid spread of propaganda, which feeds the availability heuristic. The internet makes it possible to flood the average person's daily intake of information, which aids the spread of propaganda.

One of the primary principles of propaganda is that the message must resonate with the target. Therefore, when presented with information that is within your belief structure, your bias is confirmed and you accept the propaganda. If it is outside of your network, you may initially reject the story, but the volume of information may create an availability heuristic in your mind. Over time, the propaganda becomes normalized—and even believable. It is confirmed when a fake news story is reported by the mainstream media, which has become reliant on social media for spreading and receiving news.

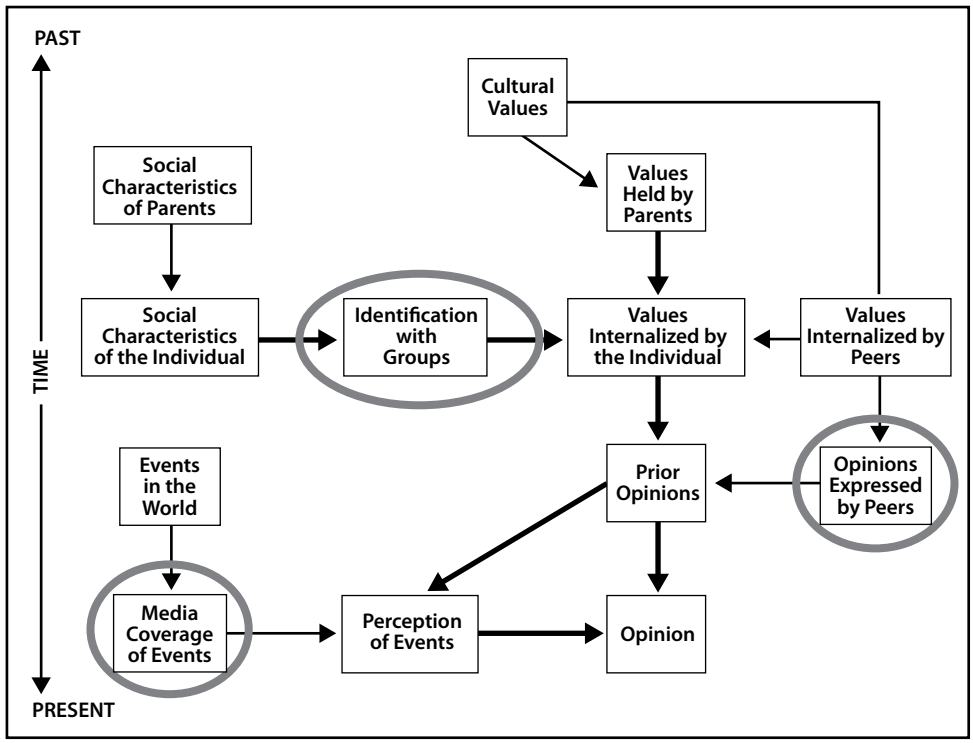


Figure 2. Model of individual opinion formation. (Reproduced by permission from Alan D. Monroe, *Public Opinion in America* [New York: Dodd, Mead, and Co., 1975], 147.)

Figure 3 maps the process of how propaganda can penetrate a network that is not predisposed to the message. This outside network is a group that is ideologically opposed to the group of true believers. The outside network is likely aware of the existing narrative but does not necessarily subscribe to the underlying beliefs that support the narrative.

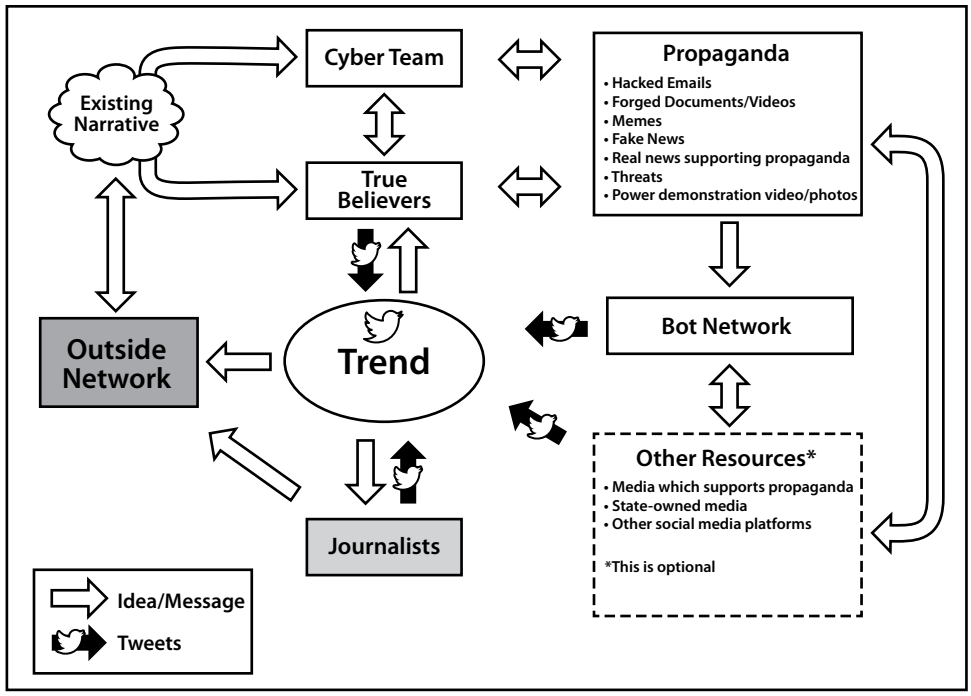


Figure 3. Process map of how propaganda spreads via the trend

Command of the trend enables the contemporary propaganda model, to create a "firehose of information" that permits the insertion of false narratives over time and at all times.[14] Trending items produce the illusion of reality, in some cases even being reported by journalists. Because untruths can spread so quickly now, the internet has created "both deliberate and unwitting propaganda" since the early 1990s through the proliferation of rumors passed as legitimate news.[15] The normalization of these types of rumors over time, combined with the rapidity and volume of new false narratives over social media, opened the door for "fake news."

The availability heuristic and the firehose of disinformation can slowly alter opinions as propaganda crosses networks by way of the trend, but

the amount of influence will likely be minimal unless it comes from a source that a nonbeliever finds trustworthy. An individual may see the propaganda and believe the message is popular because it is trending but still not buy into the message itself. Instead, the individual will likely turn to a trusted source of news to test the validity of the propaganda. Therefore, we must now analyze modern journalism to determine how command of the trend can transform propaganda from fake news to real news.

Social Networks and Social Media

Currently, 72 percent of Americans get digital news primarily from a mobile device, and people now prefer online news sources to print sources by a two-to-one ratio.[16] The news consumer now selects from an abundance of options besides a local newspaper, based on how the consumer perceives the credibility of the resource. As social media usage has become more widespread, users have become ensconced within specific, self-selected groups, which means that news and views are shared nearly exclusively with like-minded users. In network terminology, this group phenomenon is called homophily. More colloquially, it reflects the concept that "birds of a feather flock together." Homophily within social media creates an aura of expertise and trustworthiness where those factors would not normally exist. Along the lines of social networking and propaganda, people are more willing to believe things that fit into their worldview. Once source credibility is established, there is a tendency to accept that source as an expert on other issues as well, even if the issue is unrelated to the area of originally perceived expertise.[17] Ultimately, this "echo chamber" can promote the scenario in which your friend is "just as much a source of insightful analysis on the nuances of U.S. foreign policy towards Iran as regional scholars, arms control experts, or journalists covering the State Department."[18]

If social media facilitates self-reinforcing networks of like-minded users, how can a propaganda message traverse networks where there are no overlapping nodes? This link between networks is only based on that single topic and can be easily severed. Thus, to employ social media effectively as a tool of propaganda, an adversary cannot rely on individual weak links between networks. Instead, an adversary must exploit a feature within the social media platform that enables cross-network data sharing on a massive scale: the trending topics list. Trends are visible to everyone. Regardless of who follows whom on a given social media plat-

form, all users see the topics algorithmically generated by the platform as being the most popular topics at that particular moment. Given this universal and unavoidable visibility, "popular topics contribute to the collective awareness of what is trending and at times can also affect the public agenda of the community."[19] In this manner, a trending topic can bridge the gap between clusters of social networks. A malicious actor can quickly spread propaganda by injecting a narrative onto the trend list.

The combination of networking on social media, propaganda, and reliance on unverifiable online news sources introduces the possibility of completely falsified news stories entering the mainstream of public consciousness. This phenomenon, commonly called fake news, has generated significant criticism from both sides of the American political spectrum, with some labeling any contrary viewpoints fake. In reality, fake news consists of more than just bad headlines, buried ledes, or poorly sourced stories.[20] Fake news is a particular form of propaganda composed of a false story disguised as news. On social media, this becomes particularly dangerous because of the viral spread of sensationalized fake news stories.

A prime example of fake news and social media came from the most shared news stories on Facebook during the 2016 US presidential election. The source of the fake news was a supposedly patriotic American news blog called "End the Fed," a website run by Romanian businessperson Ovidiu Drobota. One story stating that the pope endorsed Donald Trump for president received over one million shares on Facebook alone, not to mention shares on Twitter.[21] Other fake news stories from that site and others received more shares in late 2016 than did traditional mainstream news sources (see figure 4).[22]

It is important to recognize that more people were exposed to those fake news stories than what is reflected in the "shares" data. In some cases, people would just see the story in a Facebook or Twitter feed; in many cases, people actively sought out news from those sources, which are fiction at best and foreign propaganda at worst. Over time, those fake news sources become trusted sources for some people. As people learn to trust those sources, legitimate news outlets become less trustworthy. A 2016 poll by Gallup showed American trust in mass media is at an all-time low.[23]

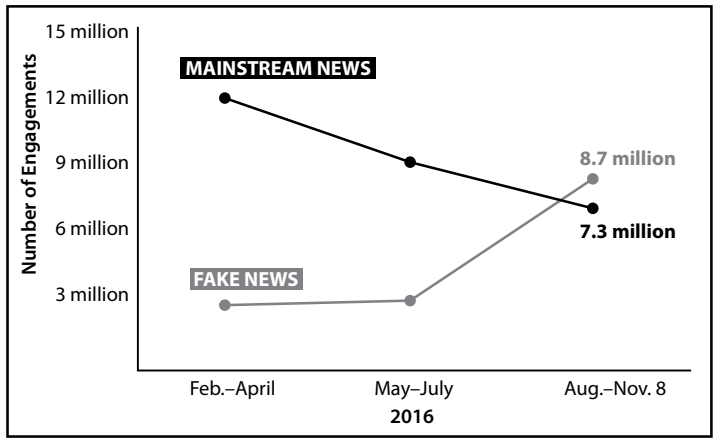


Figure 4. Total Facebook engagements for top 20 election stories

When news is tailorable to one's taste and new stories are popping up around the world every second, mainstream journalists have to change their methods to compete with other sources of news. Therefore, if social media is becoming a source for spreading news and information, journalists will try to keep up by using social media to spread their stories and to acquire information first. According to an Indiana University School of Journalism study, the most common use of social media for journalists is to check for breaking news.[24] As a result, mainstream journalists tend to use tweets as a legitimate source, especially when there is a lack of more valid or confirmed sources.[25] Overreliance on social media for breaking news can become problematic in the midst of an ongoing information operation. If an adversary takes control of a trend on Twitter, the trend is likely to be noticed by mainstream media journalists who may provide legitimacy to a false story—essentially turning fake news into real news. This is the initial setup for how social media became extremely influential via an adversary's propaganda. IS and Russia successfully manipulated social media, particularly Twitter. Although they had different objectives, the tools and techniques were similar. Both foreign actors used command of the trend to spread propaganda that influenced the emotions, opinions, and behavior of US citizens in a manner antithetical to US interests. In essence, IS and Russia hijacked social media through propaganda narratives, true believers, cyber warriors, and a bot network.

Hijacking Social Media—the Case of IS

IS could be considered either a large terrorist organization or a very fragile state with a weak army. However, the perception of IS varies. To believers, IS is a religious caliphate, but much of the rest of the world assumes it is a terrorist group that represents a perversion of faith. IS managed to master the art of manipulation because a single message simultaneously targeted potential allies and foes alike. Its use of social media is a case study in effective propaganda techniques that bolstered recruiting, increased brand recognition, and spread terror with minimal effort. It quickly became the first organization to use social media effectively to achieve its goals.

Although IS may use terrorism as a tactic, the organization behaves differently than any other terrorist organization in the world.[26] The differences are apparent in every aspect, from operations to recruiting to governing. The last factor is the key discriminator. As a descendant of al-Qaeda in Iraq, the group struggled to find its way after the death of leader Abu Musab al-Zarqawi in 2006; under the leadership of Abu Bakr al-Baghdadi the group has established clear lines of authority, taxation and educational systems, trade markets, even policing and a judiciary (covering civil, criminal, and religious complaints).[27] Gaining and holding land is just a part of what IS believes is the destiny of the organization and its followers. Certainly, the desire is to create a caliphate,[28] but its ultimate purpose is more apocalyptic in nature: IS seeks to usher in the end of the world.[29] Its members believe that their actions will bring the forces of the world to attack their caliphate and result in the imminent defeat of the infidel army in the Syrian town of Dabiq, thus triggering the end of the world and the final purge of evil.[30] IS is a revolutionary force with doomsday cult beliefs.[31]

To advance the organization's objectives, IS used messages that served to spread its propaganda on social media to a broad audience that fit within a narrative of strength for the supporter and a narrative of terror for the adversary. In other words, IS cyber warriors combined propaganda with command of the trend to accomplish three things with one message. First, they demonstrated the weakness and incompetence of the international community to fight them online and on the battlefield. Second, they injected terror into the mainstream media. Finally and most importantly, they recruited new fighters to join them on the battlefield in Iraq and Syria—and online.

Islamic State Commanding the Trend

Through a combination of ingenious marketing and cyber mastery, IS bolstered its message around the world. First, the group refined IS branding. The organization projects a very specific image to the world that affects the viewer differently based on beliefs. To a follower, the images that are shared via social media demonstrate strength and power. To the nonfollower, the images are grotesque and horrifying. In other words, no matter what IS puts out in social media the result is a win for the organization because the same message successfully targets two different groups. The amplification of those messages by creating trends on Twitter is guaranteed to get further attention once the tweet falls into the mainstream media. Thus, IS is capable of using relatively small numbers of Twitter users (see table 1) to project an aura of strength.

The method for expanding the reach of a single IS tweet or hashtag involves a network of legitimate retweets combined with bots and unwitting Twitter users. While IS does maintain a strong network of true believers, the numbers are relatively small and spread thinly across the Middle East. Therefore, IS must game the system and rig Twitter for a message to go viral. One high-tech method for creating a bot network was a mobile app called "Dawn of Glad Tidings." The app, designed by IS cyber warriors, provides updates on IS activities and spiritual guidance to the user. When users download the app, they create an account that links to their Twitter account, which then gives the app generous permissions, allowing the app to tweet using that user's account.[32] The app then retweets on behalf of the user when a master account sends an IS-branded tweet.

Over time, the hashtag generates enough tweets to start localized trends. Once the trend surfaces, it is broadcast over trend-monitoring networks, like the Arabic Twitter account @ActiveHashtags.[33] That causes the hashtag to gather more attention across the region and then be retweeted by real followers and other bot accounts. The final step in the process is when the trend goes global.

Table 1. Snapshot of Islamic State Twitter activity

Twitter-related activity studied	Related statistics
Estimated number of overt IS Twitter accounts	46,000
Number of "bot" accounts	6,216
Average number of tweets per day per user	7.3
Average number of followers	1,004
Most common year accounts created	2014
Top languages	Arabic (73%), English (18%), French (6%)
Top locations	"Islamic State," Syria, Iraq, Saudi Arabia[a]

Source: J. M. Berger and Jonathon Morgan, "The ISIS Twitter Census," Brookings Institute, accessed 20 March 2015, https://www.brookings.edu/research/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter/.

[a]Based on location-enabled users and self-defined account locations

Worldwide trends on Twitter have been a boon for IS. Creating and hijacking trends garnered attention for the group that would otherwise have gone unnoticed on social media. The peak of IS trend hijacking was during the World Cup in 2014—as one of the world's most popular sporting events, it was no surprise that the hashtag #WorldCup2014 trended globally on Twitter nonstop during the tournament. At one point though, nearly every tweet under this hashtag had something to do with IS instead of soccer. The network of IS supporters and bot accounts hijacked the trend. Because people were using the hashtag to discuss the matches and advertisers were using the trend for marketing, Twitter struggled to stop the trend and the subsequent IS propaganda effort.

In fact, IS cyber warriors and true believers foiled most of the early attempts by Twitter to stop IS from using their platform to spread propaganda. Twitter's initial reaction was to suspend accounts that violated the user terms of the agreement. The result was creative user names by IS supporters; for example, a user named @jihadISIS42 was created after @jihadISIS41 was suspended, which was set up after @jihadISIS40 was suspended.[34] Each new account demonstrated a deep dedication to the cause that, when combined with the seemingly significant presence on social media, presented the group as dominating social media.

In the case of #WorldCup2014, IS took command of the trend by hijacking, using the opportunity to push recruiting messages, and making

terror threats against the tournament venues in Brazil. Additionally, the co-opted hashtag often directed users to other hashtags in what was ultimately a successful attempt to generate worldwide trends of other IS-related themes. One successful hashtag-creation effort was #StevensHeadinObamasHands, which included memes of President Barack Obama and IS-held American journalist Steven Sotloff. The implication was that the president of the United States did not care to or was powerless to stop the murder of an American citizen. Once again, IS appeared to be disproportionately powerful because of the command of the trend.

Due to the organization's aggressive communications strategy and branding, the IS social media presence consistently outperforms similar jihadist groups in the region that have the same number of, or more, followers.[35] Unlike al-Qaeda, which largely limited its online activity to websites, IS wanted to communicate with a broader audience—it wants to communicate directly to the whole world. In addition to spreading terror threats, the appearance of the group as a powerful state appealed to a group of true believers who turned to IS as new recruits to fight in Iraq and Syria. IS used social media from 2014 to 2016 to demonstrate power, sow fear in the international audience, and recruit the true believers. All the while, they used the true believers following on social media to boost their trends on social media. However, the group currently finds itself altering its modus operandi due to the recent loss of territories in Iraq and Syria, combined with a spate of successful terrorist-style attacks in Europe. The ongoing worry for counterterrorism experts is finally beginning to come to fruition: the recruit staying home to fight instead of joining IS overseas.

After years of maintaining a significant presence on social media, IS is using Twitter less now for official communication. The reasoning is likely twofold. First, the group has lost territory in Iraq and Syria and is adjusting its strategies. Second, Twitter has removed over 600,000 IS-related accounts consisting of bots, cyber warriors, and true believers.[36] Additionally, Twitter has adjusted the program to find terror-related videos, memes, and photos soon after an account from the IS network posts the propaganda. The reasons IS seemed so powerful is that, when viewed through the lens of terrorist groups, it advertised using weaponized social media campaigns. Its intense social media presence, ghastly videos, massive

recruiting, and victories against Iraqi security forces made IS seem disproportionately stronger than it was.

In summation, IS serves as a model for any nonstate group attempting to use social media for cyber coercion. Table 2 summarizes its use of the four requirements to gain command of the trend based on the analysis within this case study.

Table 2. Islamic State case study analysis

Requirement	Example
Propaganda narratives	1. IS is strong; everyone else is weak. 2. True believers should join the cause.
True believers	Muslims believing in the caliphate of al-Baghdadi
Cyber warriors	Propaganda makers, video editors, app programmers, recruiters, spiritual leaders using low- and high-tech tools to advertise IS on social media
Bot network	Unwitting victims of spiritual-guidance app "Dawn of Glad Tidings"

At the same time IS was weaponizing Twitter, Russia was using it to simultaneously cause confusion and garner support for its invasion of Crimea. Soon, Russia's command of the trend would be used to target the United States 2016 presidential election.

Russia: Masters of Manipulation

Russia is no stranger to information warfare. The original technique of Soviet actors was through *aktivnyye meropriyatiya* (active measures) and *dezinformatsiya* (disinformation). According to a 1987 State Department report on Soviet information warfare, "active measures are distinct both from espionage and counterintelligence and from traditional diplomatic and informational activities. The goal of active measures is to influence opinions and/or actions of individuals, governments, and/or publics."[37]

In other words, Soviet agents would try to weave propaganda into an existing narrative to smear countries or individual candidates. Active measures are designed, as retired KGB General Oleg Kalugin once explained, "to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs." Editor, translator, and analyst of Russian Federation trends Michael Weiss says,

"The most common subcategory of active measures is *dezinformatsiya*, or disinformation: feverish, if believable lies cooked up by Moscow Centre and planted in friendly media outlets to make democratic nations look sinister."[38]

The techniques Russia uses today are similar to those they used during the Cold War, but dissemination is more widespread through social media. Recently, the Russian minister of defense acknowledged the existence of their cyber warriors in a speech to the Russian parliament, announcing that Russia formed a new branch of the military consisting of information warfare troops.[39] The Internet Research Agency, as it was called in 2015, now seems to be the information warfare branch he openly admitted to. This army of professional trolls' mission is to fight online. The Russian trolls have a variety of state resources at their disposal, including a vast intelligence network to assist their cyber warriors. The additional tools available to Russia also include RT (Russia Today) and Sputnik, the Kremlin-financed television news networks broadcasting in multiple languages around the world. Before the trolls begin their activities on social media, the cyber warrior hackers first provide hacked information to Wikileaks, which, according to CIA director Mike Pompeo, is a "non-state hostile intelligence service abetted by state actors like Russia."[40] In intelligence terms, WikiLeaks operates as a "cutout" for Russian intelligence operations—a place to spread intelligence information through an outside organization—similar to the Soviets' use of universities to publish propaganda studies in the 1980s.[41] The trolls then take command of the trend to spread the hacked information on Twitter, referencing WikiLeaks and links to RT news within their tweets. These Russian efforts would be impossible without an existing network of American true believers willing to spread the message. The Russian trolls and the bot accounts amplified the voices of the true believers in addition to inserting propaganda into that network. Then, the combined effects of Russian and American Twitter accounts took command of the trend to spread disinformation across networks.

The cyber trolls produced several hoaxes in the United States and Europe, like the Louisiana hoax, according to Adrian Chen in his article "The Agency" in the *New York Times Magazine*.[42] Protests of police departments throughout the United States during the summer of 2015 provided several opportunities to manipulate narratives via social media, and it is likely Russian trolls hijacked some of the Black Lives Matter–related

trends to spread disinformation and accuse journalists of failing to cover important issues.[43] The Russian trolls said the idea was to spread fear, discrediting institutions—especially American media—while making President Obama look powerless and Russian president Vladimir Putin more favorable.[44]

Several hijacked hashtags in 2015 attempted to discredit the Obama administration while spreading racist memes and hoaxes aimed at the African American community. In other words, the Russian trolls seemed to target multiple groups to generate anger and create chaos. One particularly effective Twitter hoax occurred as racial unrest fell on the University of Missouri campus that fall.

#PrayforMizzou

On the night of 11 November 2015, #PrayforMizzou began trending on Twitter.[45] The trend was a result of protests at the University of Missouri campus over racial issues; however, "news" slowly started developing within the hashtag that altered the meaning and soon shot the hashtag to the top of the trend list. The news was that the KKK was marching through Columbia and the Mizzou campus. One user, display name "Jermaine" (@Fanfan1911), warned residents, "The cops are marching with the KKK! They beat up my little brother! Watch out!" Jermaine's tweet included a picture of a black child with a severely bruised face; it was retweeted hundreds of times. Additionally, Jermaine and a handful of other users continued tweeting and retweeting images and stories of KKK and neo-Nazis in Columbia, chastising the media for not covering the racists creating havoc on campus.

Looking at Jermaine's followers, and the followers of his followers, one could observe that the original tweeters all followed and retweeted each other. Those users also seemed to be retweeted automatically by approximately 70 bots. These bots also used the trend-distribution technique, which used all of the trending hashtags at that time within their tweets, not just #PrayforMizzou. Spaced evenly, and with retweets of real people who were observing the Mizzou hashtag, the numbers quickly escalated to thousands of tweets within a few minutes. The plot was smoothly executed and evaded the algorithms Twitter designed to catch bot tweeting, mainly because the Mizzou hashtag was being used outside of that attack. The narrative was set as the trend was hijacked, and the hoax was underway.

The rapidly spreading image of a bruised little boy was generating legitimate outrage across the country and around the world. However, a quick Google image search for "bruised black child" revealed the picture that "Jermaine" attached to the tweet was a picture of an African American child who was beaten by police in Ohio over one year earlier. The image and the narrative were part of a larger plot to spread fear and distrust. It worked.

The University of Missouri student body president tweeted a warning to stay off the streets and lock doors because "KKK members were confirmed on campus." National news networks broke their coverage to get a local feed from camera crews roaming Columbia and the campus looking for signs of violence. As journalists continued to search for signs of Klan members, anchors read tweets describing shootings, stabbings, and cross burnings. In the end, the stories were all false.

Shortly after the disinformation campaign at Mizzou, @Fanfan1911 changed his display name from Jermaine to "FanFan" and the profile picture of a young black male changed to the image of a German iron cross. The next few months, FanFan's tweets were all in German and consisted of spreading rumors about Syrian refugees. Russian active measures in Europe around this time were widely reported, and the account that previously tweeted disinformation regarding Mizzou now focused on messages that were anti-Islamic, anti–European Union, and anti-German Chancellor Angela Merkel. His tweets reached a crescendo after reports of women being raped on New Year's Eve 2016. Some of the reports were false, including a high-profile case of a 13-year-old ethnic-Russian girl living in Berlin who falsely claimed that she was abducted and raped by refugees.[46] Once again, Russian propaganda dominated the narrative.[47] Similar to previous disinformation campaigns on Twitter, the Russians trolls were able to spread the information because of an underlying fear and an existing narrative that they were able to exploit. The trolls used trend-hijacking techniques in concurrence with reporting by Russian state-funded television network Russia Today. To attempt to generate more attention to the Russian anti-Merkel narrative in European media, Russian foreign minister Sergey Lavrov accused German authorities of a "politically correct cover-up" in the case of the Russian teen.[48] Because of the Russian propaganda push, the anti-immigration narrative began spreading across traditional European media.[49] In fact, a magazine in

Poland devoted an entire issue to the topic of Muslim immigration with a disturbing cover photo entitled "Islamic Rape of Europe."[50]

In addition to the German tweets, FanFan began tweeting in English again in the spring of 2016. His tweets and the tweets of other Russian trolls were spreading in America. The narrative they spread was developing a symbiotic relationship with American right-wing news organizations like Breitbart and its followers on social media—a group of true believers in the Russian propaganda narrative.

Additionally, the troll network already seeded various social media platforms with pages designed for spreading disinformation.[51] Seemingly patriotic American Facebook pages linked articles to RT, legitimate American news sources advocating a right-leaning perspective, Breitbart, right-wing conspiracy sites like InfoWars, and non-factual "news" sites like the Conservative Tribune and Gateway Pundit. The Facebook pages also linked to Russia-run sites with nothing but false news stories. Based on anti-Obama sentiment, the Facebook pages were popular among conservative users but not getting broad exposure. Before 2016, Russian active measures were also used in European elections, most notably the "Brexit" campaign. One European expert on Russia quoted in the *Atlantic* article "War Goes Viral" summarized Putin's intent as "not to make you love Putin"; instead "the aim is to make you disbelieve anything. A disbelieving, fragile, unconscious audience is much easier to manipulate."[52] Active measures enable manipulation. Smearing political candidates, hacking, the spread of disinformation, and hoaxes all contribute to a breakdown of public trust in institutions.

As the 2016 US presidential campaign began in earnest, much of the online animosity was now directed at Obama's potential successor: Hillary Clinton. She became a rallying cry for Trump supporters and a force-multiplying tool for the Russian trolls.

Influencing the 2016 Presidential Election

According to the Office of Director of National Intelligence (ODNI) Report on Russian Influence during the 2016 presidential election, "Moscow's influence campaign followed a messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state funded media, third-party intermediaries, and paid social media users, or 'trolls.' "[53] In the case of the 2016 election, Russian propaganda easily meshed with right-wing

networks known as the "alt-right" and also with supporters of Senator Bernie Sanders in the left wing of the Democratic Party. Hillary Clinton had been a target of conservative groups since she first came into the national spotlight as first lady in the 1990s.[54] Thus, groups on the left and right presented strong opposition to her candidacy in 2016, which meant Russian trolls already had a narrative to build upon and a network of true believers on social media to spread their propaganda.

In a September 2016 speech, Clinton described half of candidate Trump's supporters as "deplorables." She went on to say that the other half of Trump's supporters were just people who felt the system had left them behind, who needed support and empathy. Clearly, she was not referring to all of Trump's supporters as deplorable, but the narrative quickly changed after social media users began referring to themselves as "Deplorable" in their screen names.

Before the "basket of deplorables" comment, the trolls primarily used an algorithm to rapidly respond to a tweet from Donald Trump. Those tweets were prominently displayed directly under Trump's tweet if a user clicked on the original. Those users became powerful voices with large followings; Trump himself frequently retweeted many of those users.[55] However, after the Clinton speech, a "people search" on Twitter for "deplorable" was all one needed to suddenly gain a network of followers numbering between 3,000 and 70,000. Once again, FanFan's name changed—this time to "Deplorable Lucy"—and the profile picture became a white, middle-aged female with a Trump logo at the bottom of the picture. The FanFan follower count went from just over 1,000 to 11,000 within a few days. His original network from the Mizzou and European campaigns changed as well: tracing his follower trail again led to the same groups of people in the same network, and they were all now defined by the "Deplorable" brand. In short, they were now completely in unison with a vast network of other Russian trolls, actual American citizens, and bot accounts from both countries on Twitter. With a large network consisting of Russian trolls, true believers, and bots, it suddenly became easier to get topics trending with a barrage of tweets. The Russian trolls could employ the previously used tactics of bot tweets and hashtag hijacking, but now they had the capability to create trends.

Besides creating trends, the trolls could relay strategy under the radar using Twitter. That is to say, a message could be delivered in the form of a picture that did not include any words. The lack of words would

spread the message to the followers in a timeline, but retweets would not develop any trends—only that network of followers or someone actively observing the network saw the messages. Often, anonymous users discussed the tactics behind the trend creation on the social media site 4Chan or on the bulletin board called "/pol/" and subsequently coordinated the trend within the Deplorable Network on Twitter. The most effective trends derived from this strategy came in the days following the release of the "Access Hollywood" tape from 2005 in which Trump had made vulgar remarks.[56] The Deplorable Network distributed the corresponding strategy throughout the network to drown out negative attention to Trump on Twitter. Coinciding with the implementation of the strategy to mask anti-Trump comments on Twitter, WikiLeaks began releasing Clinton campaign chairman John Podesta's stolen emails.[57] The emails themselves revealed nothing truly controversial, but the narrative that the trending hashtag created was powerful. First, the issue of hacked emails developed into a narrative conflating Podesta's emails to the issue of Clinton's use of a private email server while she was secretary of state. The Clinton server was likely never hacked, but the problem of email loomed over her candidacy.

Secondly, the Podesta email narrative took routine issues and made them seem scandalous. The most common theme: bring discredit to the mainstream media. Podesta, like any campaign manager in modern politics, communicated with members of the press. Emails communicating with reporters were distributed via trending tweets with links to fake news websites. The fake news distorted the stolen emails into conspiracies of media "rigging" of the election to support Hillary Clinton. The corruption narrative also plagued the Democratic National Committee (DNC), which experienced a hack earlier in the year, by Russian sources and revealed by WikiLeaks.[58]

A month after the election, a man drove from his home in North Carolina to Washington, DC, to uncover the truth behind another news story he read online. He arrived at Comet Ping-Pong, a pizza restaurant, with an AR-15, prepared to free children from an underground child sex trafficking ring in the restaurant. After searching the store, he found no children. The story was a hoax. One of the emails stolen from John Podesta was an invitation to a party at the home of a friend that promised good pizza from Comet Ping Pong and a pool to entertain the kids. Fake news sites reported the email as code for a pedophilic sex party; it

was widely distributed via the trending #PodestaEmail hashtag and an associated new hashtag, #PizzaGate.

The #PizzaGate hoax, along with all of the other false and quasi-false narratives, became common within right-wing media as another indication of the immorality of Clinton and her staff. Often, the mainstream media would latch onto a story with unsavory backgrounds and false pretenses, thus giving more credibility to all of the fake news; however, the narrative from the #PizzaGate hoax followed the common propaganda narrative that the media was trying to cover up the truth and that the government failed to investigate the crimes. Ultimately, that is what drove the man to inquire into the fake news for himself.[59]

Finally, the stolen emails went beyond sharing on social media. The trend became so sensational that traditional media outlets chose to cover the Podesta email story, which gave credibility to the fake news and the associated online conspiracy theories promulgated by the Deplorable Network. The WikiLeaks release of the Podesta emails was the peak of Russian command of the trend during the 2016 election. Nearly every day #PodestaEmail trended as a new batch of supposedly scandalous hacked emails made their way into the mainstream press.

By analyzing the followers of a suspected Russian troll, a picture emerges regarding the structure of the network that was active during the 2016 election. The core group in the Deplorable Network consisted of Russian trolls and popular American right-wing accounts like Jack Posobiec, Mike Cernovich, and InfoWars editor Paul Joseph Watson. The Network also consisted of two bot accounts while the remaining nodes are individual accounts likely consisting of human-managed accounts. In total, the Deplorable Network was approximately 200,000 Twitter accounts consisting of Russian trolls, true believers, and bots. Based on my analysis, the bot network appeared to be between 16,000 and 34,000 accounts.[60] The cohesiveness of the group indicates how a coordinated effort can create a trend in a way that a less cohesive network could not accomplish. To conduct cyberattacks using social media as information warfare, an organization must have a vast network of bot accounts to take command of the trend. With unknown factors like the impact of fake news, the true results of the Russian influence operation will likely never be known. As Ellul said, experiments undertaken to gauge the effectiveness of propaganda will never work because the tests "cannot reproduce the real propaganda situation."[61] The concept itself

is marred by the fact that much of the social media support Trump received was through real American true believers tweeting. However, two numbers will stand out from the 2016 election: 2.8 million and 80,000. Hillary Clinton won the popular vote by 2.8 million votes, and Donald Trump won the electoral vote via a combination of just over 80,000 votes in three key states. One could easily make the case—as many on the left have done—that Clinton lost because of the Russian influence.[62] Conversely, one could also argue she was destined to lose because of a botched campaign combined with a growing sense of disenchantment with the American political system. However, one cannot dispute the fact that Russia launched a massive cyberwarfare campaign to influence the 2016 presidential election.[63]

For the most part, the Russian trolls became savvier with their techniques as they adapted to the influence operation in the United States. However, some users, like FanFan, were sloppy with their tradecraft and were obvious to anyone monitoring. The trolls were occasionally sloppy with their IP address locations as well. Following the first presidential debate, the #TrumpWon hashtag quickly became the number one trend globally. Using the TrendMap application, one quickly noticed that the worldwide hashtag seemed to originate in Saint Petersburg, Russia. Russian trolls gave obvious support to Donald Trump and proved that using social media could create chaos on a massive scale, discredit any politician, and divide American society.

Adrian Chen, the *New York Times* reporter who originally uncovered the troll network in Saint Petersburg in 2015, went back to Russia in the summer of 2016. Russian activists he interviewed claimed that the purpose of the trolls "was not to brainwash readers, but to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[64] The troll farm used similar techniques to drown out anti-Putin trends on Russian social media in addition to pumping out disinformation to the United States.

A Congressional Research Service Study summarized the Russian troll operation succinctly in a January 2017 report: "Cyber tools were also used [by Russia] to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the

American public about the validity of intelligence community reports, and prompting questions about the democratic process itself."[65]

For Russia, information warfare is a specialized type of war, and modern tools make social media the weapon. According to a former Obama administration senior official, Russians regard the information sphere as a domain of warfare on a sliding scale of conflict that always exists between the US and Russia.[66] This perspective was on display during a Russian national security conference "Infoforum 2016." Andrey Krutskih, a senior Kremlin advisor, compared Russia's information warfare to a nuclear bomb, which would "allow Russia to talk to Americans as equals," in the same way that Soviet testing of the atomic bomb did in 1949.[67]

Table 3. Russia case study analysis in 2016 election

Types	Examples
Propaganda narratives	• Anything discrediting to Hillary Clinton • News media hides information • Politicians are rigging the system • Global elite trying to destroy the world • Globalism is taking jobs and destroying cultures • Refugees are terrorists • Russian foreign policy is strong on antiterrorism • Democrats and some Republicans want WWIII with Russia
True believers	Alt-right, some Bernie Sanders supporters, followers of InfoWars and Breitbart, 4Chan and /pol/ users.
Cyber warriors	Hackers and professional trolls
Bot network	Large, sophisticated network that leveraged cyber warriors and true believer accounts to create the "Deplorable Network."

From 2015 to 2016, Russian trolling modus operandi took a logical path from small stories designed to create panic and sow seeds of doubt to a social media machine that IS could only imagine. In warfare strategy, narrative manipulation through social media cyber operations is the current embodiment of taking the fight directly to the people. The 2016 election proved that using social media to influence political outcomes, as opposed to violence or Cold War–like posturing, is a highly effective strategy in modern information warfare—a strategy that will likely continue as technology continues to develop and adapt to the ever-growing social media landscape as more actors gain the ability to take command of the trend.

The Future of Weaponized Social Media

Smear campaigns have been around since the beginning of politics, but this article illustrated novel techniques recently employed by a terrorist group and foreign state actor, with each attack gaining popularity and credibility after trending on Twitter. The attacks, often under the guise of a "whistleblower" campaign, make routine political actions seem scandalous. Additionally, WikiLeaks advertises that it has never published anything requiring retraction because everything it posts is supposedly authentic stolen material. Just like the Podesta email releases, several politicians and business leaders around the world have fallen victim to this type of attack.

Recall the 2015 North Korean hacking of Sony Studios. Lost in the explosive nature of the hacking story is that the fallout at the company was not because of the hacking itself but from the release of embarrassing emails from Sony senior management, as well as the salaries of every employee at Sony. The uproar over the content of the emails dominated social media, often fed by salacious stories like the RT headline: "Leaked Sony emails exhibit wealthy elite's maneuvering to get child into Ivy League school." Ultimately, Sony fired a senior executive because of the content of her emails.[68]

In another example from May 2017, nine gigabytes of email stolen from French presidential candidate Emmanuel Macron's campaign were released online and verified by WikiLeaks. Subsequently, the hashtag #MacronLeaks trended to number one worldwide. It was an influence operation resembling the #PodestaEmail campaign with a supporting cast of some of the same actors. During the weeks preceding the French election, many accounts within the Deplorable Network changed their names to support Macron's opponent, Marine LePen. These accounts mostly tweet in English and still engage in American political topics as well as French issues.[69] Some of the accounts also tweet in French, and a new network of French-tweeting bot accounts uses the same methods as the Deplorable Network to take command of the trend.

In his book *Out of the Mountains*, David Kilcullen describes a future comprising large, coastal urban areas filled with potential threats, all connected.[70] The implications of his prediction are twofold. First, networks of malicious nonstate actors can band together to hijack social media using a template similar to IS. Although these groups may not have the power to create global trends, they can certainly create chaos

with smaller numbers by hijacking trends and creating local trends. With minimal resources, a small group can create a bot network to amplify its message. Second, scores of people with exposure to social media are vulnerable to online propaganda efforts. In this regard, state actors can use the Russian playbook.

Russia will likely continue to dominate this new battlespace. It has intelligence assets, hackers, cyber warrior trolls, massive bot networks, state-owned news networks with global reach, and established networks within the countries Russia seeks to attack via social media. Most importantly, the Russians have a history of spreading propaganda. After the 2016 elections in the United States, Russian trolls again worked toward influencing European elections. Currently, Russian trolls are active in France, the Balkans, and the Czech Republic using active measures and coercive social media messages.[71] It is clear that other countries are attempting to build capabilities to match the Russian cyber troll influence.

Already, Turkey, Iran, and Venezuela are noted as having bot networks and cyber warriors similar to Russian trolls.[72] With these other states, a popular use for the trolls in the social media battlespace is to stoke nationalism and control the narrative within their own borders. For example, the fake Twitter followers of Venezuelan president Nicolás Maduro number so many that he is now the "third-most-retweeted public figure in the world, behind only the king of Saudi Arabia and the pope."[73]

With a large enough bot network, states can also control messages outside of social media using similar techniques. Manipulating search engines is called "search engine optimization," which uses bot accounts to increase the number of clicks to a particular web page after performing a search. The search engine algorithm then prioritizes that page in response to subsequent searches using the same keyword. A Google search for "ODNI Report" is illustrative: in March 2017, the top Google results were RT articles lambasting the intelligence assessment that named the Russian government as the perpetrators behind the 2016 election interference.

Techniques like search engine optimization and command of the trend will become common in future wars to sow discord and spread false information, with the aim of causing the other side to change its course of action. These online weapons should frighten every leader in a democracy. Perhaps most frightening is the Oxford Internet Institute Unit for Propaganda discovery that "hundreds of thousands of 'sleeper bots' exist

on Twitter."[74] These bots are accounts that are active but have not yet started tweeting. Researchers do not know who owns the accounts or what will trigger them. The ease of use and large numbers of active bots and sleeper bots indicate a high likelihood of social media continuing to be used for propaganda, especially as more and more state and nonstate organizations realize the impact they can make on an adversary.

Thus far, the United States response has been relatively weak. For one, the US government does not prioritize information operations the way it once did during the Cold War. When President Eisenhower started the United States Information Agency (USIA), the objective was to compete with Soviet propaganda around the world. The mission statement of USIA clarified its role: "The purpose of the United States Information Agency shall be to submit evidence to peoples of other nations by means of communication techniques that the objectives and policies of the United States are in harmony with and will advance their legitimate aspirations for freedom, progress, and peace."[75]

Knowing what we know now about Russian disinformation active measures, USIA was never truly equipped to fight an information war. The agency became a public diplomacy platform with a positive message rather than a Soviet-style campaign of negative smear tactics. Accordingly, several questions arose: should USIA spread propaganda? Should it seek out and attempt to remove negative publicity about the US? Should it slander opponents? Most importantly: should it do any or all of these things when the American public could be influenced by a message intended for an international audience?[76]

Those problems persist today because the government lacks a centralized information authority since the mission of USIA was relegated to the Department of State. Several failed attempts to counter IS on Twitter show the US government's weakness when trying to use social media as a weapon. One example is the Center for Strategic Counterterrorism Communications, created in 2010, which started the program "Think Again, Turn Away." The State department awarded a $575,046 contract to a Virginia-based consulting firm to manage the project.[77] The intent was to curb the appeal of IS by creating a counternarrative to the IS message on social media. Unfortunately, the Twitter campaign had undesirable consequences after the account sent tweets arguing the finer points of the Islamic faith with IS sympathizers. Rita Katz best summarized the failure: "In order to counter a problem, one must first study it

before adopting a solution. Had the people behind 'Think Again, Turn Away' understood jihadists' mindsets and reasons for their behavior, they would have known that their project of counter-messaging would not only be a waste of taxpayer money but ultimately be counterproductive."[78]

In the end, the "Think Again, Turn Away" campaign was almost comical as it could not communicate effectively with any audience and severely discounted the importance of its message. Jacques Ellul noted that democracies were prone to having problems with outward communication through propaganda. Because democracies rely on presenting an image of fairness and truth, "propaganda made by democracies is ineffective, paralyzed, mediocre."[79] The United States was ill equipped to combat Soviet active measures during the Cold War, and it remains unable to compete using social media as an influence operation.

Unfortunately, countering Russian influence operations has taken a partisan slant within the United States. Many downplay the Russian role in the 2016 election while others appear to be so blinded by the Russian operation that they cannot see the underlying conditions that allowed for the spread of that narrative in the first place.[80] With the two parties unable to reach a consensus on what happened or the impact of the operation, they fail to realize that as technology improves and proliferates around the world, disinformation campaigns and influence operations will become the norm. The attack in a future information war could be toward either political party and come from any of the several countries attempting to build an online army in the mold of Russia's trolls and bot network.

Conclusion

In the 1987 book *Truth Twisters*, Richard Deacon laments the future of independent thinking, as computers "could become the most dangerous hypnotic influence in the future. . . . [T]he effect of a reliance on computerology, of allowing oneself to be manipulated and controlled by it, is certainly hypnotic in that the mind allows itself to accept whatever the computer tells it."[81] He believed that such technology could lead one to commit treason without realizing any manipulation. Propaganda is a powerful tool, and, used effectively, it has been proven to manipulate populations on a massive scale. Using social media to take command of the trend makes the spread of propaganda easier than ever before for both state and nonstate actors.

Fortunately, social media companies are taking steps to combat malicious use. Facebook has been at the forefront of tech companies taking action to increase awareness of fake news and provide a process for removing the links from the website.[82] Also, although Facebook trends are less important to information warfare than Twitter trends, the website has taken measures to ensure that humans are involved in making the trends list. Furthermore, Twitter has started discreetly removing unsavory trends within minutes of their rise in popularity. However, adversaries adapt, and Twitter trolls have attempted to regain command of the trend by misspelling a previous trend once it is taken out of circulation. Still, even if the misspelled word regains a spot on the trend list, the message is diminished.

The measures enacted by Facebook and Twitter are important for preventing future wars in the information domain. However, Twitter will also continue to have problems with trend hijacking and bot networks. As demonstrated by #PrayforMizzou and #WorldCup2014, real events happening around the world will maintain popularity as well-intending users want to talk about the issues. In reality, removing the trends function could end the use of social media as a weapon, but doing so could also devalue the usability of Twitter. Rooting out bot accounts would have an equal effect since that would nearly eliminate the possibility of trend creation. Unfortunately, that would have an adverse impact on advertising firms that rely on Twitter to generate revenue for their products.

With social media companies balancing the interests of their businesses and the betterment of society, other institutions must respond to the malicious use of social media. In particular, the credibility of our press has been put into question by social media influence campaigns—those groups should respond accordingly. For instance, news outlets should adopt social media policies for their employees that encourage the use of social media but discourage them from relying on Twitter as a source. This will require a culture shift within the press and fortunately has gathered significant attention at universities researching the media's role in the influence operation. It is worth noting that the French press did not cover the content of the Macron leaks; instead, the journalists covered the hacking and influence operation without giving any credibility to the leaked information.

Finally, our elected officials must move past the partisan divide of Russian influence in the 2016 election. This involves two things: first, both parties must recognize what happened—neither minimizing nor overplaying Russian active measures. Second, and most importantly, politicians must commit to not using active measures to their benefit. Certainly, the appeal of free negative advertising will make any politician think twice about using disinformation, but the reality of a foreign influence operation damages more than just the other party, it damages our democratic ideals. Senator John McCain summarized this sentiment well at a CNN Town Hall: "Have no doubt, what the Russians tried to do to our election could have destroyed democracy. That's why we've got to pay . . . a lot more attention to the Russians."[83]

This was not the cyber war we were promised. Predictions of a catastrophic cyberattack dominated policy discussion, but few realized that social media could be used as a weapon against the minds of the population. IS and Russia are models for this future war that uses social media to directly influence people. As technology improves, techniques are refined, and internet connectivity continues to proliferate around the world, this saying will ring true: He who controls the trend will control the narrative—and, ultimately, the narrative controls the will of the people. SSQ

Notes

1. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, 11 October 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?mcubz=0/.

2. Jeremy Scott-Joynt, "What Myspace Means to Murdoch," BBC News Analysis, 19 July 2005, http://news.bbc.co.uk/2/hi/business/4697671.stm.

3. Sitaram Asur, Bernardo A. Huberman, Gabor Szabo, and Chunyan Wang, "Trends in Social Media: Persistence and Decay" (unpublished manuscript, submitted to Cornell University Library arXiv 7 February 2011), 1, https://arxiv.org/abs/1102.1402?context=physics.

4. "Blog" is short for "web log." A blog is a way to share your thoughts via the internet. A microblog is a blog with a character limit to the text.

5. Rani Molla, "Social Studies: Twitter vs. Facebook," *Bloomberg Gadfly*, 12 February 2016, https://www.bloomberg.com/gadfly/articles/2016-02-12/social-studies-comparing-twitter-with-facebook-in-charts.

6. Carole Cadwalladr, "Robert Mercer: The Big Data Billionaire Waging War on the Mainstream Media," *Guardian*, 26 February 2017, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage.

7. Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (Washington, DC: Woodrow Wilson Center Press, 2015), 138.

8. Alex Lubben, "Twitter's Users Are 15 Percent Robot, but That's Not Necessarily a Bad Thing," VICE News, 12 March 2017, https://news.vice.com/story/twitters-users-are-15-percent-robot-but-thats-not-necessarily-a-bad-thing.

9. Jacques Ellul, *Propaganda: The Formation of Men's Attitudes* (New York: Knopf, 1965), 6.

10. Eric Hoffer, *The True Believer: Thoughts on the Nature of Mass Movements* (New York: Harper and Row, 1951), 105.

11. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 132.

12. Ellul, 85.

13. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 87.

14. Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Report PE-198-OSD (Santa Monica, CA: RAND, 2016), 4, https://www.rand.org/pubs/perspectives/PE198.html.

15. Garth Jowett and Victoria O'Donnell, *Propaganda & Persuasion*, 5th ed. (Thousand Oaks, CA: SAGE, 2012), 159.

16. Katerina Eva Matsa and Kristine Lu, "10 Facts about the Changing Digital News Landscape," Pew Research Center, 14 September 2016, http://www.pewresearch.org/fact-tank/2016/09/14/facts-about-the-changing-digital-news-landscape/.

17. Jowett and O'Donnell, *Propaganda & Persuasion*, 300.

18. Tom Hashemi, "The Business of Ideas Is in Trouble: Re-injecting Facts into a Post-truth World," *War on the Rocks*, 9 December 2016, https://warontherocks.com/2016/12/the-business-of-ideas-is-in-trouble-re-injecting-facts-into-a-post-truth-world/.

19. Asur, Huberman, Szabo, and Wang, "Trends in Social Media," 1.

20. *Merriam-Webster Dictionary Online*, s.v. "lede," accessed 10 October 2017, https://www.merriam-webster.com/dictionary/lede. "The introductory section of a news story that is intended to entice the reader to read the full story."

21. Tess Townsend, "The Bizarre Truth behind the Biggest Pro-Trump Facebook Hoaxes," Inc.com, 21 November 2016, https://www.inc.com/tess-townsend/ending-fed-trump-facebook.html.

22. Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook," BuzzFeed News, 16 November 2016, https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.qwWdA0G8G#.fcEv1Qono.

23. Art Swift, "Americans' Trust in Mass Media Sinks to New Low," Gallup, 14 September 2016, http://news.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx.

24. Andrea Peterson, "Three Charts that Explain how U.S. Journalists Use Social Media," *Washington Post*, 6 May 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/05/06/three-charts-that-explain-how-u-s-journalists-use-social-media/?utm_term=.9cdd82cb8fa7.

25. Weimann, *Terrorism in Cyberspace*, 138.

26. Audrey Kurth Cronin, "ISIS Is Not a Terrorist Group," *Foreign Policy* (March/April 2015), https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group.

27. Stephen M. Walt, "ISIS as Revolutionary State," *Foreign Policy* (November/December 2015): 42, https://www.belfercenter.org/publication/isis-revolutionary-state.

28. Caliphate is defined as "a form of Islamic government led by a—a person considered a political and religious successor to the Islamic prophet, Muhammad, and a leader of the entire Muslim community. Source: Wadad Kadi and Aram A. Shahin, "Caliph, caliphate," in *The Princeton Encyclopedia of Islamic Political Thought*, ed. Gerhard Bowering, Patricia Crone, Wadad Kadi, Devin J. Stewart, Muhammad Qasim Zaman, and Mahan Mirza (Princeton, NJ: Princeton University Press, 2013), 81–86, http://www.jstor.org/stable/j.ctt1r2g6m.8.

29. Graeme Wood, "What ISIS Really Wants," *Atlantic*, March 2015, 3, https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/.

30. Dabiq is also the name of the ISIS magazine, which is available electronically and spread via social media.

31. Walt, "ISIS as Revolutionary State," 43.

32. J. M. Berger, "How ISIS Games Twitter," *Atlantic*, 16 June 2014, https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

33. Ibid.

34. "Terrorist Use of Social Media: Policy and Legal Challenges," roundtable forum (Washington, DC: Council on Foreign Relations, 14 October 2015).

35. Berger, "How ISIS Games Twitter."

36. Carleton English, "Twitter Continues to Wage its Own War against ISIS," *New York Post*, 21 March 2017, http://nypost.com/2017/03/21/twitter-continues-to-wage-its-own-war-against-isis/.

37. United States Department of State, report, *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87* (Washington, DC: Bureau of Public Affairs, 1987), viii.

38. Natasha Bertrand, "It Looks Like Russia Hired Internet Trolls to Pose as Pro-Trump Americans," *Business Insider*, 27 July 2016, http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7.

39. Vladimir Isachenkov, "Russia Military Acknowledges New Branch: Info Warfare Troops," AP News, 22 February 2017, https://www.apnews.com/8b7532462dd0495d9f756c9ae7d2ff3c.

40. Richard Gonzalez, "CIA Director Pompeo Denounces WikiLeaks as 'Hostile Intelligence Service,' " NPR, 23 April 2017, http://www.npr.org/sections/thetwo-way/2017/04/13/523849965/cia-director-pompeo-denounces-wikileaks-as-hostile-intelligence-service.

41. Malcolm Nance, *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election* (New York: Skyhorse Publishing, 2016), Kindle edition, 1,839.

42. Adrian Chen, "The Agency," *New York Times Magazine*, 2 June 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html. On 11 September 2014, the small town of St. Mary Parish, Louisiana, was thrown briefly into a panic when residents began hearing reports through text, social media, and on local television stations that a nearby chemical plant fire was spreading toxic fumes that would soon endanger the whole town. The entire narrative was based on falsified—but very real looking—online news stories, hashtag manipulation, and mass texts (SMS) to various numbers with the local area code and dialing prefix. The actual source for the news was not the chemical factory; it was a nondescript building in St. Petersburg, Russia, where an army of online cyber-warrior trolls seeks to distribute false information.

43. Statement of Clint Watts, Foreign Policy Research Institute fellow, in "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," testimony before the Senate Intelligence Committee, 115th Cong., 1st sess., 30 March 2017, https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf.

44. Chen, "The Agency."

45. Because of the Adrian Chen article, I observed particular tweeting patterns of certain individuals involved in a hoax on the campus of the University of Missouri that seemed to match the methods of the Russian trolls interviewed by Chen. I mention only one particular user in this article, but I also monitored a dozen or so accounts that contributed to that hoax. Each account followed a pattern that also happened to align with noted Russian influence operations in Europe and eventually in the US presidential election. I describe that transition in the article. From those accounts, I built a database of suspected Russian bot accounts to build a network map. The Mizzou hoax was a trend hijacking effort launched by actors who later proved to match the Russian modus operandi of using cyber trolls originally observed by Adrian Chen and confirmed by the Office of the Director of National Intelligence (ODNI) report and Foreign Policy Research Institute fellow Clint Watts in his testimony before the Senate Intelligence Committee (note 43).

46. Nadine Schmidt and Tim Hume, "Berlin Teen Admits Fabricating Migrant Gang-Rape Story, Official Says," CNN, 1 February 2016, http://www.cnn.com/2016/02/01/europe/germany-teen-migrant-rape-false/index.html.

47. Judy Dempsey, "Russia's Manipulation of Germany's Refugee Problems," Carnegie Europe, 28 January 2016, http://carnegieeurope.eu/strategiceurope/?fa=62611.

48. Schmidt and Hume, "Berlin Teen Admits Fabricating Migrant Gang-Rape Story."

49. Barbara Tasch, "'The Aim Is to Weaken the West': The Inside Story of How Russian Propagandists Are Waging War on Europe," *Business Insider*, 2 February 2017, http://www.businessinsider.com/russia-propaganda-campaign-weakening-europe-2017-1?r=UK&IR=T.

50. Harriet Sherwood, "Polish Magazine's 'Islamic Rape of Europe' Cover Sparks Outrage," 18 February 2016, https://www.theguardian.com/world/2016/feb/18/polish-magazines-islamic-of-europe-cover-sparks-outrage.

51. Chen, "The Agency."

52. Robinson Meyer, "War Goes Viral: How Social Media Is Being Weaponized across the World," *Atlantic*, 18 October 2016, https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/.

53. Office of the Director of National Intelligence (ODNI), Intelligence Community Assessment Report, *Assessing Russian Activities and Intentions in Recent US Elections*, 6 January 2017, ii, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

54. Hanna Rosin, "Among the Hillary Haters," *Atlantic*, 1 March 2015, 63, https://www.theatlantic.com/magazine/archive/2015/03/among-the-hillary-haters/384976/.

55. K. Thor Jensen, "Inside Donald Trump's Twitter-Bot Fan Club," *New York Magazine*, 15 June 2016, http://nymag.com/selectall/2016/06/inside-donald-trumps-twitter-bot-fan-club.html.

56. David A. Farenthold, "Trump Recorded Having Extremely Lewd Conversation about Women in 2005," *Washington Post*, 8 October 2016, https://www.washingtonpost.com/politics/trump-recorded-having-extremely-lewd-conversation-about-women-in-2005/2016/10/07/3b9ce776-8cb4-11e6-bf8a-3d26847eeed4_story.html.

57. "The Podesta Emails," Politico LiveBlog, accessed 6 December 2016, http://www.politico.com/live-blog-updates/2016/10/john-podesta-hillary-clinton-emails-wikileaks-000011.

58. ODNI Report, 2.

59. Faiz Siddiqui and Susan Svrluga, "N.C. Man Told Police He Went to D.C. Pizzeria with Gun to Investigate Conspiracy Theory," *Washington Post*, 5 December 2017, https://www.washingtonpost.com/news/local/wp/2016/12/04/d-c-police-respond-to-report-of-a-man-with-a-gun-at-comet-ping-pong-restaurant/?utm_term=.c33057f66007.

60. This count is based on analysis of the followers of followers of suspected troll accounts and bots. The study was conducted 15 March 2016. The number of accounts appears to have reduced dramatically since May, following the French election, implying that Twitter suspended some of the accounts. Unfortunately, software limitations prevent this analysis from being more accurate. Additionally, it is nearly impossible to derive the exact number of Russian accounts from that network using my available resources.

61. Ellul, *Propaganda*, 6.

62. Many on the left have mischaracterized the attack as "Russian hacking of the election," which has in turn conflated the issue of the John Podesta email theft with a hacking of the actual election systems. To be clear: there is no evidence of any sort of hack on any ballot-counting systems, only evidence outlined in this paper of two hacks (Democratic National Committee and Podesta) combined with an influence/information operation.

63. ODNI Report, 1.

64. Adrian Chen, "The Real Paranoia-Inducing Purpose of Russian Hacks," *New Yorker*, 27 July 2016, https://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks.

65. Catherine Theohary and Cory Welt, "Russia and the U.S. Presidential Election," CRS Report no. IN10635 (Washington, DC: Congressional Research Service, 2017).

66. David Ignatius, "Russia's Radical New Strategy for Information Warfare," *Washington Post*, 18 January 2017, https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.da53e31d7aaa.

67. Ibid.

68. "Ex-Sony Chief Amy Pascal Acknowledges She Was Fired," NBCNews.com, 12 February 2015, https://www.nbcnews.com/storyline/sony-hack/ex-sony-chief-amy-pascal-acknowledges-she-was-fired-n305281.

69. The political left in the United States seems to have a large group of bot accounts forming around the "Resist" movement. It is unclear whether those accounts are foreign cyber warriors or bots, but external actors can certainly feed off the underlying narratives and tap into existing networks of true believers.

70. David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013), 231.

71. Anthony Faiola, "As Cold War Turns to Information War, a New Fake News Police Combats Disinformation," *Washington Post*, 22 January 2017, https://www.washingtonpost.com/world/europe/as-cold-war-turns-to-information-war-a-new-fake-news-police/2017/01/18/9bf49ff6-d80e-11e6-a0e6-d502d6751bc8_story.html?utm_term=.7c99cc2fadd5.

72. Meyer, "War Goes Viral."

73. Ibid.

74. Cadwalladr, "Robert Mercer: The Big Data," 1.8.

75. Malcolm Mitchell, *Propaganda, Polls, and Public Opinion: Are the People Manipulated?* (Englewood Cliffs, NJ: Prentice-Hall, 1977), 12.

76. Ibid., 13.

77. Rebecca Carroll, "The State Department Is Fighting with ISIL on Twitter." Defense One, 25 June 2014, http://www.defenseone.com/technology/2014/06/state-department-fighting-isil-twitter/87286/.

78. Rita Katz, "The State Department's Twitter War with ISIS Is Embarrassing," *Time*, 16 September 2014, http://time.com/3387065/isis-twitter-war-state-department/.

79. Ellul, *Propaganda*, 241.

80. Adrian Chen, "The Propaganda about Russian Propaganda," *New Yorker*, 1 December 2016, https://www.newyorker.com/news/news-desk/the-propaganda-about-russian-propaganda.

81. Richard Deacon, *The Truth Twisters* (London: Macdonald, 1987), 95.

82. Michelle Castillo, "Facebook Found Fake Accounts Leaking Stolen Info to Sway Presidential Election," CNBC.com, 27 April 2017, https://www.cnbc.com/2017/04/27/facebook-found-efforts-to-sway-presidential-election-elect-trump.html.

83. Eric Bradner, "At CNN Town Hall, McCain and Graham Give Their View of Trump's Presidency so Far," CNN, 2 March 2017, http://www.cnn.com/2017/03/01/politics/john-mccain-lindsey-graham-town-hall/index.html.

Disclaimer

JTRIG tools and techniques

(Redirected from JTRIG CITD - Covert Internet Technical Development)

Overview | JTRIG Capabilities | Contacts

[edit] JTRIG tools

Contents

We don't update this page anymore, it became somewhat of a Chinese menu for effects operations. Information is now available for JTRIG staff at [[1]]

[edit] Understanding this page

Tools and techniques are developed by various teams within JTRIG. We like to let people know when we have something that we can think we can use, but we also don't want to oversell our capability.

For this reason, each tool indicates its current status. We may put up experimental tools or ones that are still in development so you know what we are working on, and can approach JTRIG with any new ideas. But experimental tools by their nature will be unreliable, if you raise expectations or make external commitments before speaking to us you will probably end up looking stupid.

Most of our tools are fully operational, tested and reliable. We will indicate when this is the case; however there can be reasons why our tools won't work for some operational requirements (eg if it exploits a provider specific vulnerability). There may also be legal restrictions.

So please come and speak to JTRIG operational staff early in your operational planning process.

[edit] Current Priorities

Capability Development Priorities can be fond by following the link below

- CapDev Priorities (Discover)

[edit] Engineering

Tool/System	Description	Status	Contacts
Cerberus Statistics Collection	Collects on-going usage information about how many users utilise JTRIG's UIA capability, what sites are the most frequently visited etc. This is in order to provide JTRIG infrastucture and ITServices management information statistics.	OPERATIONAL	JTRIG Software Developers
JTRIG RADIANT SPLENDOUR	is a 'Data Diode' connecting the CERBERUS network with GCNET	OPERATIONAL	JTRIG Software Developers
ALLIUM ARCH	JTRIG UIA via the Tor network.	OPERATIONAL	JTRIG Infrastructure Team
ASTRAL PROJECTION	Remote GSM secure covert internet proxy using TOR hidden services.	OPERATIONAL	JTRIG Infrastructure Team
TWILIGHT ARROW	Remote GSM secure covert internet proxy using VPN services.	OPERATIONAL	JTRIG Infrastructure Team
SPICE ISLAND	JTRIG's new Infrastructure. FOREST WARRIOR, FRUIT BOWL, JAZZ FUSION and other JTRIG systems will form part of the SPICE ISLAND infrastructure	DEV	JTRIG Infrastructure Team
POISON ARROW	Safe Malware download capability.	DESIGN	JTRIG Infrastructure Team
FRUIT BOWL	CERBERUS UIA Replacement and new tools infrastructure – Primary Domain for Generic User/Tools Access and TOR split into 3 sub-systems.	DESIGN	JTRIG Infrastructure Team
NUT ALLERGY	JTRIG Tor web browser - Sandbox IE replacement and FRUIT BOWL sub-system	PILOT	JTRIG Infrastructure Team
BERRY TWISTER	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team
BERRY TWISTER+	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team m]
BRANDY SNAP	JTRIG UIA contingency at Scarborough.	IMPLEMENTATION	JTRIG Infrastructure Team
WIND FARM	R&D offsite facility.	DESIGN	JTRIG Infrastructure Team
CERBERUS	JTRIG's legacy UIA desktop, soon to be replaced with FOREST WARRIOR.	OPERATIONAL	JTRIG Infrastructure Team
BOMBAYROLL	JTRIG's legacy UIA standalone capability.	OPERATIONAL	JTRIG Infrastructure Team
JAZZ FUSION	BOMBAY ROLL Replacement which will also incorporate new collectors – Primary Domain for Dedicated Connections split into 3 sub-systems.	IMPLEMENTATION	JTRIG Infrastructure Team
COUNTRY FILE	A sub-system of JAZZ FUSION	OPERATIONAL	JTRIG Infrastructure Team
TECHNO VIKING	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team
JAZZ FUSION+	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team
BUMBLEBEE DANCE	JTRIG Operational VM/TOR architecture	OPERATIONAL	JTRIG Infrastructure Team
AIR BAG	JTRIG Laptop capability for field operations.	OPERATIONAL	JTRIG Infrastructure Team
EXPOW	GCHQ's UIA capability provided by JTRIG.	OPERATIONAL	JTRIG Infrastructure Team
AXLE GREASE	The covert banking link for CPG	OPERATIONAL	JTRIG Infrastructure Team
POD RACE	JTRIG'S MS update farm	DESIGN	JTRIG Infrastructure Team
WATCHTOWER	GCNET -> CERBERUS Export Gateway Interface System	OPERATIONAL	JTRIG Software Developers
REAPER	CERBERUS -> GCNET Import Gateway Interface System	OPERATIONAL	JTRIG Software Developers
DIALd	External Internet Redial and Monitor Daemon	OPERATIONAL	JTRIG Software Developers
FOREST WARRIOR	Desktop replacement for CERBERUS	DESIGN	JTRIG Infrastructure Team
DOG HANDLER	JTRIG's development network	DESIGN	JTRIG Infrastructure Team
DIRTY DEVIL	JTRIG'S research network	DESIGN	JTRIG Infrastructure Team

[edit] Collection

Tool	Description	Contacts	Status
AIRWOLF	YouTube profile, comment and video collection.	[redacted]	Beta release.
ANCESTRY	Tool for discovering the creation date of yahoo selectors.	JTRIG Software Developers	Fully Operational.
BEARTRAP	Bulk retrieval of public BEBO profiles from member or group ID.	JTRIG Software Developers	Fully Operational.
BIRDSONG	Automated posting of Twitter updates.	JTRIG Software Developers	Decomissioned. Replaced by SYLVESTER.
BIRDSTRIKE	Twitter monitoring and profile collection. Click here for the User Guide.	JTRIG Software Developers	Fully Operational.
BUGSY	Google+ collection (circles, profiles etc.)	Tech Leads: [redacted]	In early development.
DANCING BEAR	obtains the locations of WiFi access points.	[Tech Lead: [redacted] Expert User: [redacted]	Fully Operational.
DEVILS HANDSHAKE	ECI Data Technique.	[Tech Lead: [redacted] Expert User: [redacted]	Fully Operational.
DRAGON'S SNOUT	Paltalk group chat collection.	Tech Leads: [redacted]	Beta release.
EXCALIBUR	acquires a Paltalk UID and/or email address from a Screen Name.	JTRIG Software Developers	Fully operational (against current Paltalk version)
FATYAK	Public data collection from LinkedIn.	[Tech Lead: [redacted]	In development
FUSEWIRE	Provides 24/7 monitoring of Vbulliten forums for target postings/online activity. Also allows staggered postings to be made.	JTRIG Software Developers	
GLASSBACK	Technique of getting a targets IP address by pretending to be a spammer and ringing them. Target does not need to answer.	JTRIG Software Developers	Fully operational.
GODFATHER	Public data collection from Facebook.	[Tech Lead: [redacted]	Fully operational.
GOODFELLA	Generic framework for public data collection from Online Social Networks.	[Tech Lead: [redacted]	In Development (Supports RenRen and Xing).
HACIENDA	is a port scanning tool designed to scan an entire country or city. It uses GEOFUSION to identify IP locations. Banners and content are pulled back on certain ports. Content is put into the EARTHLING database, and all other scanned data is sent to GNE and is available through GLOBAL SURGE and Fleximart.	NAC HACIENDA Taskers	Fully operational.
ICE	is an advanced IP harvesting technique.	JTRIG Software Developers	
INSPECTOR	Tool for monitoring domain information and site availability.	JTRIG Software Developers	Fully Operational.
LANDING PARTY	Tool for auditing dissemination of VIKING PILLAGE data.	JTRIG Software Developers	Fully Operational.

MINIATURE HERO	Active skype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists.	JTRIG Software Developers	Fully operational, but note usage restrictions.
MOUTH	Tool for collection for downloading a user's files from Archive.org.	JTRIG Software Developers	Fully Operational.
MUSTANG	provides covert access to the locations of GSM cell towers.	[Tech Lead: [redacted] Expert User: [redacted]	Fully Operational.
PHOTON TORPEDO	A technique to actively grab the IP address of an MSN messenger user.	Tech Lead: [redacted]	Operational, but usage restrictions.
RESERVOIR	Facebook application allowing collection of various information.	JTRIG Software Developers	Fully operational, but note operational restrictions.
SEBACIUM	An ICTR developed system to identify P2P file sharing activity of intelligence value. Logs are accessible via DIRTY RAT.	[Tech Lead: [redacted] Expert User: [redacted]	
SILVER SPECTER	Allows batch Nmap scanning over TOR	JTRIG Software Developers	In Development
SODAWATER	A tool for regularly downloading gmail messages and forwarding them onto CERBERUS mailboxes	JTRIG Software Developers	Fully Operational.
SPRING BISHOP	Find private photographs of targets on Facebook.	Tech Lead: [redacted]	
SYLVESTER	Framework for automated interaction / alias management on online social networks.	Tech Lead: [redacted]	In Development.
TANNER	A technical programme allowing operators to log on to a JTRIG website to grab IP addresses of Internet Cafe's.	JTRIG OSO	Replaced by HAVOK.
TRACER FIRE	An Office Document that grabs the targets Machine info, files, logs, etc and posts it back to GCHQ.	[redacted] TRACER FIRE JTRIG	In Development.
VIEWER	A programme that (hopefully) provides advance tip off of the kidnappers IP address for HMG personnel.	[Tech Lead: [redacted] Expert User: [redacted]	Operational, but awaiting field trial.
VIKING PILLAGE	Distributed network for the automatic collection of encrypted/compressed data from remotely hosted JTRIG projects.	PILLAGE JTRIG Software Developers	Operational
TOP HAT	A version of the MUSTANG and DANCING BEAR techniques that allows us to pull back Cell Tower and WiFi locations targeted against particular areas.	[Tech Lead: [redacted]	In development.

[edit] Effects Capability

JTRIG develop the majority of effects capability in GCHQ. A lot of this capability is developed on demand for specific operations and then further developed to provide weaponised capability.

Don't treat this like a catalogue. If you don't see it here, it doesn't mean we can't build it. If you involve the JTRIG operational teams at the start of your operation, you have more of a chance that we will build something for you.

For each of our tools we have indicated the state of the tool. We only advertise tools here that are either ready to fire or very close to being ready (operational requirements would re-prioritise our development). Once again, involve the JTRIG operational teams early.

Tool	Description	Status	Contacts
ANGRY PIRATE	is a tool that will permanently disable a target's account on their computer.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
ARSON SAM	is a tool to test the effect of certain types of PDU SMS messages on phones / network. It also includes PDU SMS Dumb Fuzz testing.	Ready to fire (Not against live targets, this is a R&D Tool).	[Tech Lead: [redacted] Expert User:]
BUMPERCAR+	is an automated system developed by JTRIG CITD to support JTRIG BUMPERCAR operations. BUMPERCAR operations are used to disrupt and deny Internet-based terror videos or other material. The technique employs the services provided by upload providers to report offensive materials.	Ready to fire.	JTRIG Software Developers
BOMB BAY	is the capability to increase website hits/rankings.	In Development.	[Tech Lead: [redacted]
BADGER	mass delivery of email messaging to support an Information Operations campaign	Ready to fire.	JTRIG OSO
BURLESQUE	is the capability to send spoofed SMS text messages.	Ready to fire.	JTRIG OSO
CANNONBALL	is the capability to send repeated text messages to a single target.	Ready to fire.	JTRIG OSO
CLEAN SWEEP	Masquerade Facebook Wall Posts for individuals or entire countries	Ready to fire (SIGINT sources required)	[Tech Lead: [redacted] Expert User:
CLUMSY BEEKEEPER	Some work in progress to investigate IRC effects.	NOT READY TO FIRE.	Tech Lead: [redacted] Expert User : [redacted]
CHINESE FIRECRACKER	Overt brute login attempts against online forums	Ready to fire.	FIRECRACKER
CONCRETE DONKEY	is the capability to scatter an audio message to a large number of telephones, or repeatedly bomb a target number with the same message.	In development.	[redacted]
DEER STALKER	Ability to aid-geolocation of Sat Phones / GSM Phones via a silent calling to the phone.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
GATEWAY	Ability to artificially increase traffic to a website	Ready to fire.	JTRIG OSO
GAMBIT	Deployable pocket-sized proxy server	In-development	JTRIG OSO
GESTATOR	amplification of a given message, normally video, on popular multimedia websites (Youtube).		[Tech Lead: ?; Expert User: [redacted]
GLITTERBALL	Online Gaming Capabilities for Sensitive Operations. Currently Second Life.	In development.	
IMPERIAL BARGE	For connecting two target phone together in a call.	Tested.	[Tech Lead: [redacted] Expert User: [redacted]
PITBULL	Capability, under development, enabling large scale delivery of a tailored message to users of Instant Messaging services.	In development.	
POISONED DAGGER	Effects against Gigatribe. Built by ICTR, deployed by JTRIG.		Tech Lead: [redacted]

PREDATORS FACE	Targeted Denial Of Service against Web Servers.		Tech Lead: [redacted]
ROLLING THUNDER	Distributed denial of service using P2P. Built by ICTR, deployed by JTRIG.		Tech Lead: [redacted]
SCARLET EMPEROR	Targeted denial of service against targets phones via call bombing.	Ready to fire.	JTRIG Software Developers
SCRAPHEAP CHALLENGE	Perfect spoofing of emails from Blackberry targets.	Ready to fire, but see constraints.	[redacted]
SERPENTS TONGUE	for fax message broadcasting to multiple numbers.	In redevelopment.	[Tech Lead: [redacted] Expert User: [redacted]
SILENT MOVIE	Targeted denial of service against SSH services.	Ready to fire.	[Tech Lead: [redacted]
SILVERBLADE	Reporting of extremist material on DAILYMOTION.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SILVERFOX	List provided to industry of live extremist material files hosted on FFUs.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SILVERLORD	Disruption of video-based websites hosting extremist content through concerted target discovery and content removal.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SKYSCRAPER	Production and dissemination of multimedia via the web in the course of information operations.	Ready to fire.	[Tech Lead: Section X; Expert Users: Language Team]
SLIPSTREAM	Ability to inflate page views on websites	Ready to fire.	JTRIG OSO
STEALTH MOOSE	is a tool that will Disrupt target's Windows machine. Logs of how long and when the effect is active.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User:]
SUNBLOCK	Ability to deny functionality to send/receive email or view material online.	Tested, but operational limitations.	[Tech Lead: Section X; Expert User: [redacted]
Swamp donkey	is a tool that will silently locate all predefined types of file and encrypt them on a targets machine.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
TORNADO ALLEY	is a delivery method (Excel Spreadsheet) that can silently extract and run an executable on a target's machine.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
UNDERPASS	Change outcome of online polls (previously known as NUBILO)	In development.	[Tech Lead: Section X; Expert User: [redacted]
VIPERS TONGUE	is a tool that will silently Denial of Service calls on a Satellite Phone or a GSM Phone.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
WARPATH	Mass delivery of SMS messages to support an Information Operations campaign	Ready to fire.	JTRIG OSO

[edit] Work Flow Management

Tool	Description	Contacts
HOME PORTAL	A central hub for all JTRIG Cerberus tools	JTRIG Software Developers
CYBER COMMAND CONSOLE	A centralised suite of tools, statistics and viewers for tracking current operations across the Cyber community.	JTRIG Software Developers
NAMEJACKER	A web service and admin console for the translation of usernames between networks. For use with gateways and other such technologies.	JTRIG Software Developers

[edit] Analysis Tools

Tool	Description	Contacts
BABYLON	is a tool that bulk queries web mail addresses and verifies whether they can be signed up for. A green tick indicates that the address is currently in use. Verification can currently be done for Hotmail and Yahoo.	JTRIG Software Developers
CRYOSTAT	is a JTRIG tool that runs against data held in NEWPIN. It then displays this data in a chart to show links between targets.	JTRIG Software Developers
ELATE	is a suite of tools for monitoring target use of the UK auction site eBay (www.ebay.co.uk). These tools are hosted on an Internet server, and results are retreived by encrypted email.	JTRIG Software Developers
PRIMATE	is a JTRIG tool that aims to provides the capability to identify trends in seized computer media data and metadata.	JTRIG Software Developers
JEDI	JTRIG will shortly be rolling out a JEDI pod to every desk of every member of an Intelligence Production Team. The challenge is to scale up to over 1,200 users whilst remaining agile, efficent and responsive to customer needs.	[Tech Lead: [redacted] Expert User: [redacted]
JILES	is a JTRIG bespoke web browser.	[Tech Lead: [redacted] Expert User:]
MIDDLEMAN	is a distributed real-time event aggregation, tip-off and tasking platform utilised by JTRIG as a middleware layer.	JTRIG Software Developers
OUTWARD	is a collection of DNS lookup, WHOIS Lookup and other network tools.	JTRIG Software Developers
TANGLEFOOT	is a bulk search tool which queries a set of online resources. This allows analysts to quickly check the online presence of a target.	JTRIG Software Developers
SCREAMING EAGLE	is a tool that processes kismet data into geolocation information	
SLAMMER	is a data index and repository that provides analysts with the ability to query data collected from the Internet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts etc.	JTRIG Software Developers

[edit] Databases

Tool	Description	Contacts
BYSTANDER	is a categorisation database accessed via web service.	JTRIG Software Developers
CONDUIT	is a database of C2C identifiers for Intelligence Community assets acting online, either under alias or in real name.	JTRIG Software Developers
NEWPIN	is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data.	JTRIG Software Developers
QUINCY	is an enterprise level suite of tools for the exploitation of seized media.	[Tech Lead: [redacted] Expert Users: [redacted]

[edit] Forensic Exploitation

Tool	Description	Contacts
BEARSCRAPE	can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box.	[Tech Lead: [redacted] Expert User:]
SFL	The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution.	[Tech Lead: [redacted] Expert User:
Snoopy	is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK.	[Tech Lead: [redacted]
MobileHoover	is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, Snoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin.	[Tech Lead: [redacted]
Nevis	is a tool developed by NTAC to search disk images for signs of possible Encryption products. CMA have further developed this tool to look for signs of Steganography.	[Tech Lead: [redacted]

[edit] Techniques

Tool	Description	Contacts
CHANGELING	Ability to spoof any email address and send email under that identity	JTRIG OSO
HAVOK	Real-time website cloning technique allowing on-the-fly alterations	JTRIG OSO
MIRAGE		JTRIG OSO
SHADOWCAT	End-toEnd encrypted access to a VPS over SSH using the TOR network	JTRIG OSO
SPACE ROCKET	is a programme covering insertion of media into target networks. CRINKLE CUT is a tool developed by ICTR-CISA to enable JTRIG track images as part of SPACE ROCKET.	Tech Lead: [redacted] Expert User:
RANA	is a system developed by ICTR-CISA providing CAPTCHA-solving via a web service on CERBERUS. This is intended for use by BUMPERCAR+ and possibly in future by SHORTFALL but anyone is welcome to use it.	Tech Lead: [redacted] Expert Use
LUMP	A system that finds the avatar name from a SecondLife AgentID	JTRIG Software Developers
GURKHAS SWORD	Beaconed Microsoft Office Documents to elicite a targets IP address.	JTRIG Software Developers

[edit] Shaping and Honeypots

Tool	Description	Contacts
DEADPOOL	URL shortening service	JTRIG OSO
HUSK	Secure one-to-one web based dead-drop messaging platform	JTRIG OSO
LONGSHOT	File-upload and sharing website	JTRIG OSO
MOLTEN-MAGMA	CGI HTTP Proxy with ability to log all traffic and perform HTTPS Man in the Middle.	JTRIG Software Developers
NIGHTCRAWLER	Public online group against dodgy websites	JTRIG OSO
PISTRIX	Image hosting and sharing website	JTRIG OSO
WURLITZER	Distribute a file to multiple file hosting websites.	[redacted]

JTRIG Logo.png

Category: JTRIG

JTRIG Tools and Techniques

A transcription of the catalog of exploit tools posted on The Intercept.

JTRIG tools

We don't update this page anymore, it became somewhat of a Chinese menu for effects operations. Information is now available for JTRIG staff at [1]

Understanding this page

Tools and techniques are developed by various teams within JTRIG. We like to let people know when we have something that we can think we can use, but we also don't want to oversell our capability.

For this reason, each tool indicates its current status. We may put up experimental tools or ones that are still in development so you know what we are working on, and can approach JTRIG with any new ideas. But experimental tools by their nature will be unreliable, if you raise expectations or make external commitments before speaking to us you will probably end up looking stupid.

Most of our tools are fully operational, tested and reliable. We will indicate when this is the case, however there can be reasons why our tools won't work for some operational requirements (eg if it exploits a provider specific vulnerability). There may also be legal restrictions.

So please come and speak to JTRIG operational staff early in your operational planning process.

Engineering

Tool/System	Description	Status	Contacts
Cerberus Statistics Collection	Collects on-going usage information about how many users utilise JTRIG's UIA capability, what sites are the most frequently visited etc. This is in order to provide JTRIG infrastucture and ITServices management information statistics.	OPERATIONAL	JTRIG Software Developers
JTRIG RADIANT SPLENDOUR	is a 'Data Diode' connecting the CERBERUS network with GCNET	OPERATIONAL	JTRIG Software Developers
ALLIUM ARCH	JTRIG UIA via the Tor network.	OPERATIONAL	JTRIG Infrastructure Team
ASTRAL PROJECTION	Remote GSM secure covert internet proxy using TOR hidden services.	OPERATIONAL	JTRIG Infrastructure Team
TWILIGHT ARROW	Remote GSM secure covert internet proxy using VPN services.	OPERATIONAL	JTRIG Infrastructure Team
SPICE ISLAND	JTRIG's new Infrastructure. FOREST WARRIOR, FRUIT BOWL, JAZZ FUSION and other JTRIG systems will form part of the SPICE ISLAND infrastructure	DEV	JTRIG Infrastructure Team
POISON ARROW	Safe Malware download capability.	DESIGN	JTRIG Infrastructure Team
FRUIT BOWL	CERBERUS UIA Replacement and new tools infrastructure - Primary Domain for Generic User/Tools Access and TOR split into 3 sub-systems.	DESIGN	JTRIG Infrastructure Team
NUT ALLERGY	JTRIG Tor web browser - Sandbox IE replacement and FRUIT BOWL sub-system	PILOT	JTRIG Infrastructure Team
BERRY TWISTER	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team

BERRY TWISTER+	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team
BRANDY SNAP	JTRIG UIA contingency at Scarborough.	IMPLEMENTATION	JTRIG Infrastructure Team
WIND FARM	R&D offsite facility.	DESIGN	JTRIG Infrastructure Team
CERBERUS	JTRIG's legacy UIA desktop, soon to be replaced with FOREST WARRIOR.	OPERATIONAL	JTRIG Infrastructure Team
BOMBAYROLL	JTRIG's legacy UIA standalone capability.	OPERATIONAL	JTRIG Infrastructure Team
JAZZ FUSION	BOMBAY ROLL Replacement which will also incorporate new collectors - Primary Domain for Dedicated Connections split into 3 sub-systems.	IMPLEMENTATION	JTRIG Infrastructure Team
COUNTRY FILE	A sub-system of JAZZ FUSION	OPERATIONAL	JTRIG Infrastructure Team
TECHNO VIKING	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team
JAZZ FUSION+	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team
BUMBLEBEE DANCE	JTRIG Operational VM/TOR architecture	OPERATIONAL	JTRIG Infrastructure Team
AIR BAG	JTRIG Laptop capability for field operations.	OPERATIONAL	JTRIG Infrastructure Team
EXPOW	GCHQ's UIA capability provided by JTRIG.	OPERATIONAL	JTRIG Infrastructure Team
AXLE GREASE	The covert banking link for CPG	OPERATIONAL	JTRIG Infrastructure Team
POD RACE	JTRIG'S MS update farm	DESIGN	JTRIG Infrastructure Team
WATCHTOWER	GCNET -> CERBERUS Export Gateway Interface System	OPERATIONAL	JTRIG Software Developers
REAPER	CERBERUS -> GCNET Import Gateway Interface System	OPERATIONAL	JTRIG Software Developers
DIALd	External Internet Redial and Monitor Daemon	OPERATIONAL	JTRIG Software Developers
FOREST WARRIOR	Desktop replacement for CERBERUS	DESIGN	JTRIG Infrastructure Team
DOG HANDLER	JTRIG's development network	DESIGN	JTRIG Infrastructure Team
DIRTY DEVIL	JTRIG'S research network	DESIGN	JTRIG Infrastructure Team

Collection

Tool	Description	Contacts	Status
AIRWOLF	YouTube profile, comment and video collection.	[redacted]	Beta release.
ANCESTRY	Tool for discovering the creation date of yahoo selectors.	JTRIG Software Developers	Fully Operational.
BEARTRAP	Bulk retrieval of public BEBO profiles from member or group ID.	JTRIG Software Developers	Fully Operational.
BIRDSONG	Automated posting of Twitter updates.	JTRIG Software Developers	Decommissioned. Replaced by SYLVESTER.
BIRDSTRIKE	Twitter monitoring and profile collection. Click here for the User Guide.	JTRIG Software Developers	Fully Operational.
BUGSY	Google+ collection (circles, profiles etc.)	Tech Leads: [redacted]	In early development.
DANCING BEAR	obtains the locations of WiFi access points.	[Tech Lead: [redacted] Expert User: [redacted]	Fully Operational.
DEVIL'S HANDSHAKE	ECI Data Technique.	[Tech Lead: [redacted] Expert User: [redacted]	Fully Operational.
DRAGON'S SNOUT	Paltalk group chat collection.	Tech Leads: [redacted]	Beta release.
EXCALIBUR	acquires a Paltalk UID and/or email address from a Screen Name.	JTRIG Software Developers	Fully Operational (against current Paltalk version)
FATYAK	Public data collection from LinkedIn.	[Tech Lead: [redacted]	In Development.
FUSEWIRE	Provides 24/7 monitoring of Vbulliten forums for target postings/online activity. Also allows staggered postings to be made.	JTRIG Software Developers	
GLASSBACK	Technique of getting a targets IP address by pretending to be a spammer and ringing them. Target does not need to answer.	JTRIG Software Developers	Fully Operational.
GODFATHER	Public data collection from Facebook.	[Tech Lead: [redacted]	Fully Operational.
GOODFELLA	Generic framework for public data collection from Online Social Networks.	[Tech Lead: [redacted]	In Development (Supports RenRen and Xing).

HACIENDA	is a port scanning tool designed to scan an entire country or city. It uses GEOFUSION to identify IP locations. Banners and content are pulled back on certain ports. Content is put into the EARTHLING database, and all other scanned data is sent to GNE and is available through GLOBAL SURGE and Fleximart.	NAC HACIENDA Taskers	Fully Operational.
ICE	is an advanced IP harvesting technique.	JTRIG Software Developers	
INSPECTOR	Tool for monitoring domain information and site availability	JTRIG Software Developers	Fully Operational.
LANDING PARTY	Tool for auditing dissemination of VIKING PILLAGE data.	JTRIG Software Developers	Fully Operational.
MINIATURE HERO	Active skype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists.	JTRIG Software Developers	Fully operational, but note usage restrictions.
MOUTH	Tool for collection for downloading a user's files from Archive.org.	JTRIG Software Developers	Fully Operational.
MUSTANG	provides covert access to the locations of GSM cell towers.	[Tech Lead: [redacted] Expert User: [redacted]	Fully Operational.
PHOTON TORPEDO	A technique to actively grab the IP address of MSN messenger user.	Tech Lead: [redacted]	Operational, but usage restrictions.
RESERVOIR	Facebook application allowing collection of various information.	JTRIG Software Developers	Fully operational, but note operational restrictions.
SEBACIUM	An ICTR developed system to identify P2P file sharing activity of intelligence value. Logs are accessible via DIRTY RAT.	[Tech Lead: [redacted] Expert User: [redacted]	
SILVER SPECTER	Allows batch Nmap scanning over Tor.	JTRIG Software Developers	In Development.
SODAWATER	A tool for regularly downloading gmail messages and forwarding them onto CERBERUS mailboxes	JTRIG Software Developers	Fully Operational.

SPRING BISHOP	Find private photographs of targets on Facebook.	Tech Lead: [redacted]	
SYLVESTER	Framework for automated interaction / alias management on online social networks.	Tech Lead: [redacted]	In Development.
TANNER	A technical programme allowing operators to log on to a JTRIG website to grab IP addresses of Internet Cafe's.	JTRIG OSO	Replaced by HAVOK.
TRACER FIRE	An Office Document that grabs the targets Machine info, files, logs, etc and posts it back to GCHQ.	[redacted] TRACER FIRE JTRIG	In Development.
VIEWER	A programme that (hopefully) provides advance tip off of the kidnappers IP address for HMG personnel.		Operational, but awaiting field trial.
VIKING PILLAGE	Distributed network for the automatic collection of encrypted/compressed data from remotely hosted JTRIG projects.	PILLAGE JTRIG Software Developers	Operational.
TOP HAT	A version of the MUSTANG and DANCING BEAR techniques that allows us to pull back Cell Tower and WiFi locations targeted against particular areas.	[Tech Lead: [redacted]	In Development.

Effects Capability

JTRIG develop the majority of effects capability in GCHQ. A lot of this capability is developed on demand for specific operations and then further developed to provide weaponised capability.

Don't treat this like a catalogue. If you don't see it here, it doesn't mean we can't build it. If you involve the JTRIG operational teams at the start of your operation, you have more of a chance that we will build something for you.

For each of our tools we have indicated the state of the tool. We only advertise tools here that are either ready to fire or very close to being ready (operational requirements would re-prioritise our development). Once again, involve the JTRIG operational teams early.

Tool	**Description**	**Status**	**Contacts**
ANGRY PIRATE	is a tool that will permanently disable a target's account on their computer.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
ARSON SAM	is a tool to test the effect of certain types of PDU SMS messages on phones / network. It also includes PDU SMS Dumb Fuzz testing	Ready to fire (Not against live targets, this is a R&D Tool).	[Tech Lead: [redacted] Expert User:]

BUMPERCAR+	is an automated system developed by JTRIG CITD to support JTRIG BUMPERCAR operations. BUMPERCAR operations are used to disrupt and deny Internet-based terror videos or other materials. The technique employs the services provided by upload providers to report offensive materials.	Ready to fire.	JTRIG Software Developers
BOMB BAY	is the capability to increase website hits/rankings.	In Development.	[Tech Lead: [redacted]
BADGER	mass delivery of email messaging to support an Information Operations campaign	Ready to fire.	JTRIG OSO
BURLESQUE	is the capabiltiy to send spoofed SMS text messages.	Ready to fire.	JTRIG OSO
CANNONBALL	is the capability to send repeated text messages to a single target.	Ready to fire.	JTRIG OSO
CLEAN SWEEP	Masquerade Facebook Wall Posts for individuals or entire countries.	Ready to fire (SIGINT sources required)	[Tech Lead: [redacted] Expert User:
CLUMSY BEEKEPER	Some work in progress to investigate IRC effects.	NOT READY TO FIRE.	[Tech Lead: [redacted] Expert User: [redacted]
CHINESE FIRECRACKER	Overt brute login attempts against online forums	Ready to fire.	FIRECRACKER
CONCRETE DONKEY	is the capability to scatter an audio message to a large number of telephones, or repeatedly bomb a target number with the same message.	In development.	[redacted]
DEER STALKER	Ability to aid-geolocation of Sat Phones / GSM Phones via a silent calling to the phone.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
GATEWAY	Ability to artificially increase traffic to a website.	Ready to fire.	JTRIG OSO
GAMBIT	Deployable pocket-sized proxy server	In-development	JTRIG OSO
GESTATOR	amplification of a given message, normally video, on popular multimedia websites (Youtube).		[Tech Lead: ?, Expert User: [redacted]
GLITTERBALL	Online Gaming Capabilities for Sensitive Operations. Currently Second Life.	In development.	
IMPERIAL BARGE	For connecting two target phone together in a call.	Tested.	[Tech Lead: [redacted] Expert User: [redacted]

PITBULL	Capability, under development, enabling large scale delivery of a tailored message to users of Instant Messaging services.	In development.	
POISONED DAGGER	Effects against Gigatribe. Built by ICTR, deployed by JTRIG.		Tech Lead: [redacted]
PREDATORS FACE	Targeted Denial Of Service against Web Servers.		Tech Lead: [redacted]
ROLLING THUNDER	Distributed denial of service using P2P. Built by ICTR, deployed by JTRIG.		Tech Lead: [redacted]
SCARLET EMPEROR	Targeted denial of service against targets phones via call bombing.	Ready to fire.	JTRIG Software Developers
SCRAPHEAP CHALLENGE	Perfect spoofing of emails from Blackberry targets.	Ready to fire, but see constraints.	[redacted]
SERPENTS TONGUE	for fax message broadcasting to multiple numbers.	In redevelopment.	[Tech Lead: [redacted] Expert User: [redacted]
SILENT MOVIE	Targeted denial of service against SSH services.	Ready to fire.	Tech Lead: [redacted]
SILVERBLADE	Reporting of extremist material on DAILYMOTION.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SILVERFOX	List provided to industry of live extremist material files hosted on FFUs.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SILVERLORD	Disruption of video-based websites hosting extremist content through concerted target discovery and content removal.	Ready to fire.	[Tech Lead: [redacted] Expert User: [redacted]
SKYSCRAPER	Production and dissemination of multimedia via the web in the course of information operations.	Ready to fire.	[Tech Lead: Section X; Expert Users: Language Team]
SLIPSTREAM	Ability to inflate page views on websites	Ready to fire.	JTRIG OSO
STEALTH MOOSE	is a tool that will Disrupt target's Window's machine. Logs of how long and when the effect is active.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User:]
SUNBLOCK	Ability to deny functionality to send/receive email or view material online.	Tested, but operational limitations.	[Tech Lead: Section X; Expert User [redacted]
Swamp donkey	is a tool that will silently locate all predefined types of file and encrypt them on a targets machine.	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]
TORNADO ALLEY	is a delivery method (Excel Spreadsheet) that can silently extract and run an executable on	Ready to fire (but see target restrictions).	[Tech Lead: [redacted] Expert User: [redacted]

	a target's machine.		
UNDERPASS	Change outcome of online polls (previously known as NUBILO)	In development.	[Tech Lead: Section X; Expert User [redacted]
VIPERS TONGUE	is a tool that will silently Denial of Service calls on a Satellite Phone or a GSM Phone.	Ready to fire (but see target restrictions).	[Tech Lead: Section X; Expert User [redacted]
WARPATH	Mass delivery of SMS messages to support an Information Operations campaign	Ready to fire.	JTRIG OSO

Work Flow Management

Tool	Description	Contacts
HOME PORTAL	A central hub for all JTRIG Cerberus Tools	JTRIG Software Developers
CYBER COMMAND CONSOLE	A centralised suite of tools, statistics and viewers for tracking current operations across the Cyber community.	JTRIG Software Developers
NAMEJACKER	A web service and admin console for the translation of usernames between networks. For use with gateways and other such technologies.	JTRIG Software Developers

Analysis Tools

Tool	Description	Contacts
BABYLON	is a tool that bulk queries web mail addresses and verifies whether they can be signed up for. A green tick indicates that the address is currently in use. Verification can currently be done for Hotmail and Yahoo.	JTRIG Software Developers
CRYOSTAT	is a JTRIG tool that runs against data held in NEWPIN. It then displays this data in a chart to show links between targets.	JTRIG Software Developers
ELATE	is a suite of tools for monitoring target use of the UK auction site eBay (www.ebay.co.uk). These tools are hosted on an Internet server, and results are retreived by encrypted email.	JTRIG Software Developers
PRIMATE	is a JTRIG tool that aims to provides the capability to identify trends in seized computer media data and metadata.	JTRIG Software Developers
JEDI	JTRIG will shortly be rolling out a JEDI pod to every desk of every member of an Intelligence Production Team. The challenge is to scale up to over 1,200 users whilst remaining agile, efficent and responsive to customer needs.	[Tech Lead: [redacted] Expert User: [redacted]
JILES	is a JTRIG bespoke web browser.	[Tech Lead: [redacted] Expert User:]
MIDDLEMAN	is a distributed real-time event aggregation, tip-off and tasking platform utilised by JTRIG as a middleware layer.	JTRIG Software Developers
OUTWARD	is a collection of DNS lookup, WHOIS Lookup and other network tools.	JTRIG Software Developers

TANGLEFOOT	is a bulk search tool which queries a set of online resources. This allows analysts to quickly check the online presence of a target.	JTRIG Software Developers
SCREAMING EAGLE	is a tool that processes kismet data into geolocation information	
SLAMMER	is a data index and repository that provides analysts with the ability to query data collected from the Internet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts etc.	JTRIG Software Developers

Databases

Tool	Description	Contacts
BYSTANDER	is a categorisation database accessed via web service.	JTRIG Software Developers
CONDUIT	is a database of C2C identifiers for Intelligence Community assets acting online, either under alias or in real name.	JTRIG Software Developers
NEWPIN	is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data.	JTRIG Software Developers
QUINCY	is an enterprise level suite of tools for the exploitation of seized media.	[Tech Lead: [redacted] Expert User: [redacted]

Forensic Exploitation

Tool	Description	Contacts
BEARSCRAPE	can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box.	[Tech Lead: [redacted] Expert User:]
SFL	The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution.	[Tech Lead: [redacted] Expert User: [redacted]
Snoopy	is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK.	[Tech Lead: [redacted]
MobileHoover	is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, Snoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin.	[Tech Lead: [redacted]
Nevis	is a tool developed by NTAC to search disk images for signs of possible Encryption products. CMA have further developed this tool to look for signs of Steganography.	[Tech Lead: [redacted]

Techniques

Tool	Description	Contacts
CHANGELING	Ability to spoof any email address and send email under that identify	JTRIG OSO

HAVOK	Real-time website cloning techniques allowing on-the-fly alterations.	JTRIG OSO
MIRAGE		JTRIG OSO
SHADOWCAT	End-toEnd encrypted access to a VPS over SSH using the TOR network	JTRIG OSO
SPACE ROCKET	is a programme covering insertion of media into target networks. CRINKLE CUT is a tool developed by ICTR-CISA to enable JTRIG track images as part of SPACE ROCKET.	Tech Lead: [redacted] Expert User:
RANA	is a system developed by ICTR-CISA providing CAPTCHA-solving via a web service on CERBERUS. This is intended for use by BUMPERCAR+ and possibly in future by SHORTFALL but anyone is welcome to use it.	Tech Lead: [redacted] Expert User:
LUMP	A system that finds the avatar name from a SecondLife AgentID	JTRIG Software Developers
GURKHAS SWORD	Beaconed Microsoft Office Documents to elicite a targets IP address.	JTRIG Software Developers

Shaping and Honeypots

Tool	**Description**	**Contacts**
DEADPOOL	URL shortening service	JTRIG OSO
HUSK	Secure one-on-one web based dead-drop messaging platform	JTRIG OSO
LONGSHOT	File-upload and sharing website	JTRIG OSO
MOLTEN-MAGMA	CGI HTTP Proxy with ability to log all traffic and perform HTTPS Man in the Middle.	JTRIG OSO
NIGHTCRAWLER	Public online group against dodgy websites	JTRIG OSO
PISTRIX	Image hosting and sharing website	JTRIG OSO
WURLITZER	Distribute a file to multiple file hosting websites.	[redacted]

TOP SECRET STRAP1

Tor: Overview of Existing Techniques (15 minutes)

[redacted]

ICTR-NE

Previous Work/Current Techniques

ICTR-related techniques

- Identification of events by content
- Tor node dictionary generation – available from web site
- HOMING TROLL – Bridge discovery prototype that feeds dictionary
- Statistical deanonymisation research (MCR)
- NEWTONS CRADLE (JTRIG)
- TRIBAL CARNEM (with CT)
- EPIC FAIL (CT)
- Bulk traffic logging
- QUICK ANT - Low latency deanonymisation. Prototype under evaluation.
- Introducing timing patterns – report available
- Hidden service investigation – report available
- Shaping research – some initial experiments.
- Some extraction of hidden service domain names from passive events.
- Tor implementation analysis (contract task)

Also some work (through contract) on Freenet.

ICTR-NE Goals for 2012/13

Our plans at present are:

- Tor deanonymisation – collaboration with MCR and JTRIG
- Tor shaping – with JTRIG
- Contract: next stage of Tor Implementation Analysis

- ICTR-CISA: record hidden service hostnames (*.onion) in NATURAL SELECTION.

… so REMATION II fits in well.

Any questions?

Reference: Ideas (2011)

- Maintain knowledge of Tor network – Pullthrough from NE?
- Log Tor events into HAKIM for target discovery – TR-FSP
- Build tool to implement low latency attack? – ICTR
- Collecting traffic at exit nodes to feed passive SIGINT - JTRIG
- Testing of MCR passive deanonymisation technique. – MCR/JTRIG/ICTR
- Active injection and detection of timing patterns (probably following test of MCR technique) – ICTR/JTRIG/MCR
- Herding of targets through our exit nodes (THEMP) – ICTR/JTRIG
- Bulk logging of hidden service onion addresses (possibly only those hosting web sites) – experiment carried out by ICTR
- Characterisation of hidden web servers by passive analysis – ICTR?
- Characterisation of hidden web servers by web crawling – ICTR?
- Identification of IP addresses hosting hidden services – ICTR?
- Ongoing use/maintenance of TRIBAL CARNEM - CT
- Find TDIs that appear on Tor and non-tor IP addresses (EPIC FAIL) - CT
- Understanding Tor circuit creation and destruction – ICTR contract
- Understanding future developments in Tor – ICTR contract?
- Spotting private Tor networks – ICTR?
- TorChat investigation? – ICTR?

Reference: Data Sources

- Tor node consensus (obtained by Tor client) – UNCLASSIFIED
- Information on Tor Bridges – CONFIDENTIAL
- Collection from exit nodes – SECRET
- Passive intercept (SECRET/TOP SECRET)
  - SSL events in cloud(s)
  - Tor packet logging (ICTR system)
  - Content exiting Tor network