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