Zersetzungsprogramm des britischen Nachrichtendienstes - Joint Threat Research Intelligence Group

Die **Joint Threat Research Intelligence Group** (**JTRIG**) ist eine Einheit des britischen Nachrichtendienstes GCHQ.[1] Die Existenz von JTRIG wurde im Zuge der Globalen Überwachungs- und Spionageaffäre als Teil der Enthüllungen vom früheren NSA-Auftragnehmer Edward Snowden bekannt.[2]

Inhaltsverzeichnis

Auftrag

Der Zuständigkeitsbereich des JTRIG umfasst "schmutzige Tricks", um Feinde “zu verleugnen, zu stören, zu zersetzen und zu zerstören”, indem sie “diskreditiert” werden, Fehlinformationen platziert werden und ihre Kommunikation stillzulegen versucht wird.[2]

Einsätze

Beim „Cognitive Hacking“ greifen Geheimdienste aktiv in demokratische Prozesse ein, um diese zu beeinflussen, z. B. durch die Manipulation von Online-Abstimmungen. Laut GCHQ sind alle Operationen mit den britischen Gesetzen vereinbar.[3]

Im Jahr 2011 leitete das JTRIG einen DoS-Angriff auf das Aktivistennetzwerk Anonymous.[1] Andere JTRIG-Ziele beinhalteten das Nuklearprogramm des Iran und die Taliban in Afghanistan.[2]

Vom JTRIG durchgeführte Kampagnen lassen sich größtenteils in zwei Kategorien einteilen; Cyberattacken und Propaganda-Bemühungen. Die Propaganda-Bestrebungen nutzen „Massenbenachrichtigungen“ und das „Streuen von Gerüchten“ in sozialen Netzwerken, wie z. B. in Twitter, Flickr, Facebook und YouTube.[2] „False flag“-Operationen wurden ebenfalls vom JTRIG gegen Ziele eingesetzt.[2]

Es handelt sich um eine breitflächige Diskreditierung der Netzkommunikation. Da diese Methoden auch gegen Personen verwendet werden, die keinerlei Gefahr für die nationale Sicherheit darstellen, handelt es sich um eine klare Grenzverschiebung.[4]

Ein Computervirus namens Ambassadors Reception wurde vom GCHQ „in einer Vielfalt von unterschiedlichen Bereichen“ eingesetzt und in Folien als „sehr effektiv“ beschrieben. Der Virus kann “sich selbst verschlüsseln, alle E-Mails löschen, alle Dateien verschlüsseln, [und den] Bildschirm erzittern lassen”, wenn er an Gegner gesendet wird.[2] Der Virus kann außerdem verhindern, dass sich der Nutzer an seinem Rechner anmelden kann.[2]

Die Folien enthüllten außerdem die Nutzung von „Honigfallen“ sexueller Natur von britischen Agenten.[2] Ein identifiziertes Ziel wird „an einen bestimmten Ort im Internet, oder zu einem physischen Ort“ gelockt, um dort “ein freundliches Gesicht” zu treffen, mit dem Ziel denjenigen zu diskreditieren.[2] Eine “Honigfalle” wird auf den Folien als „sehr erfolgreich“ betrachtet, „wenn sie funktioniert“.[2]

Beweisquelle: https://de.wikipedia.org/wiki/Joint_Threat_Research_Intelligence_Group

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)

2.18 *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

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.

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