Proposed information-processing influences. The alternative side to this debate suggests that errors are caused by generally adaptive information-processing styles and short-cuts. This research has spread from the attributional field into that of human judgment and decision making in the more general sense. Researchers have pointed out many weaknesses in human cognition, but this paper describes only three which have been highlighted by D. Kahneman and A. Tversky (Psychological Review, 1973, 237-251). This is because these three information-processing factors may represent the more general processes that underlie many more specific cognitive errors.

Kahneman and Tversky suggest that people habitually use certain cognitive short-cuts to make their decisions and judgments quickly and effectively. Generally these strategies, or heuristics, are effective, but their use may also lead to errors. The first of these heuristics is termed judgment by availability, where people's judgments about the relative frequency of objects or the likelihood of events may be influenced by the relative availability of these objects or events, availability referring to the accessibility of items in perception, memory, or imagination. The second heuristic is termed judgment by representativeness or similarity, where an individual's judgment of the probability that two events are related depends very much on the degree to which these events have features that are similar to each other. The final information-processing strategy which can lead to errors is judgment by anchoring and adjustment. Here, individuals are said to make judgments by starting with an initial value or position which is then insufficiently adjusted to account for new/incoming information--this is one way in which erroneous beliefs may be maintained even in the face of disconfirming information.

Conclusions

This paper describes three areas of cognitive social psychological research that bear on the question of errors in everyday human judgment and inference and consequently on the examination of errors in conclusions about the occurrence of psi in spontaneous settings. The research described does not as yet form any coherent theory of human error and indeed, may not be new to parapsychologists. However, this paper is intended to serve three functions: (1) to integrate some findings of relevance to parapsychology and present them in a way that shows their context within psychological research on human judgmental error; (2) to inform or remind parapsychologists of the various ways in which false-positive or false-negative conclusions about the occurrence of psi may be reached, which may help in eventually identifying mistaken conclusions about the operation of psi and consequently enhancing the quality of data on the occurrence of psi; and (3) to stress that while there is some emphasis in parapsychology on mistaken conclusions that psi has occurred, psychological research on human error logically cuts both ways, and can aid in the identification of false-positive and false-negative conclusions about the occurrence of psi.

ANOMALOUS HUMAN-COMPUTER INTERACTION (AHCI): TOWARDS AN UNDERSTANDING OF WHAT CONSTITUTES AN ANOMALY (OR, HOW TO MAKE FRIENDS AND INFLUENCE COMPUTERS)

K. Morgan (Dept. of Psychology, University of Edinburgh,
7 George Square, Edinburgh EH8 9JZ, Scotland)

This paper is an attempt to clarify in what manner a genuine anomaly can be distinguished from an incident explicable by known physical means. It also tries to exemplify the various methods that could be used to simulate an anomalous human-computer interaction (AHCI). This paper does not dwell in any more than a superficial manner upon the psychology involved in manipulating observers which would allow the described physical strategies to be carried out. That would demand a paper in its own right.

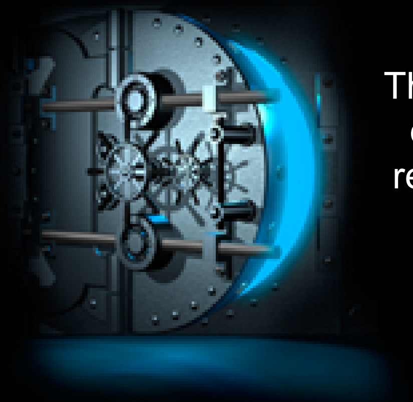
Part of the research being carried out at the Koestler Chair and other institutions is the investigation of anomalous human-computer interaction. As with any area of parapsychological research there always exists the danger of the researcher mistaking a normally explicable phenomenon as an anomaly. This paper was written to help people who are confronted by an unusual happening on a computer to evaluate the situation and to be aware of the possibility of there being normal methods of simulating almost any anomaly.

The various categories into which both simulated and genuine anomalies could fall can be separated into the following:

(1) Human. The majority of so-called anomalies might be found to be caused by the users' ignorance of their own computer system or aspects of it. This, coupled with the human trait of forcing unconnected events into meaningful patterns, might explain many anomalies.

(2) Software Anomaly. The methods of achieving the simulation of a software (nonhardware-based) anomaly can be broken down into the following categories:

(a) Replacement of the target program. The target program or process is exchanged for an amended version that contains the extra "feature" that will become the "anomaly."



(b) Adjusting or amending the target program or process. In this scenario the target process is amended at the same time or very shortly before the "anomaly." This would of course demand the knowledge of the specification of the software being used at the target site.

(c) Breaches in computer/organizational security both prior to and simultaneously with anomaly. These are often a necessary prerequisite of any of the above software anomalies. The breach in security could even be from a remote site, via a computer communication link that has access to the target system. The use of interpreted languages or online debugging (disassembling) tools makes this reasonably easy.

(3) Hardware Anomaly. This section covers any physical effect that occurs to an item of computer machinery (but not to the logic controlling it). These "effects" could often take the form of either repairing or destroying an item of equipment. These items could be anything from a personal electronic belonging (e.g., an electronic watch) to a computer's storage device.

(a) Replacement. In this scenario an exact duplicate of the target is prepared and exchanged for the target item when the opportunity arises. The duplicate has some extra "feature" which will be used by the false anomalist to simulate the required anomaly.

(b) Adjustment/destruction--"live." To adjust or amend an item of equipment is not as difficult as it might appear. Much computing equipment is sensitive to one or many of the following environmental influences: weak magnetic fields, physical force (e.g., bending), exposure for long periods to strong sunlight, contact with sharp objects, extreme humidity, temperatures outside the tolerated range, contact with static electricity, and any substances or object making contact with a recording or electrically conductive surface.

(c) Breaches in computer/organizational security before or simultaneously with anomaly. In contrast to the previous scenarios, simulating hardware anomalies requires the physical presence of the false anomalist or environmental influence in order to achieve the anomaly.

(4) External to Computer System. Such things as electrical mains fluctuations are a possible example of natural "disasters," and if the fluctuation coincided with some other meaningful event the users might decide that an anomaly had occurred which had a correlation with that meaningful event, thus starting local lore about this false correlation.

Methods of Avoiding Computer-Based Fraudulent Anomalies

Examples of new technology that might help alleviate the above-mentioned problems are

(1) WORMS (write once read many times) optical disks. These (at present) are noneditable and are immune to "grubby thumbs," magnetic fields, and static. They are therefore much better potential psi-corruption targets than the currently favorite floppy disk, especially if the target data on the disk are well encrypted and the disk uniquely identified.

(2) Optical fiber cables. This makes data transmission line monitoring or adjustment much more complex.

(3) Automated technical advisers for computer-based security. These can rapidly and thoroughly analyze a large and highly complex system specification for security weaknesses. They are only as good as the level of detail or accuracy in the specification and the expertise of their user.

(4) Gypsy verification environments & (5) Program analysis tools. Both of these methods could be useful in the analysis of a piece of code that has been in an "anomaly." Again, they are subject to the same weaknesses discussed under the previous heading.

(6) Cryptographic methods. These can be highly effective in preventing access to information, provided a sufficiently good encryption method is selected.

(7) Shielding. Simple shielding of vdu screen emission can eliminate the chance of a computer screen being reconstituted outside the system confines.

Conclusion

This paper has tried to portray the various scenarios that could be misinterpreted as an "anomalous" human-computer interaction (AHCI). It also tried to show that there are conceptual patterns that allow AHCI anomalies to be categorized, along with their possible fraudulent explanations. It is hoped that armed with such a method of categorization experimenters may be able better to record and evaluate the intriguing field of AHCI. In such evaluations it may be more cost effective to create a means of detecting a fraudulent anomaly rather than to proof a system against every possible threat. A highly motivated false anomalist with large financial and time resources might be able to create fraudulent anomalies, regardless of the tightest precautions. Experimenters might therefore find it helpful to adopt an experimental condition where no one star "makes or breaks" the results. By using large "anonymous" source groups the incentive for any one individual to create false anomalies might be greatly reduced.

STATISTICAL ISSUES AND METHODS*

WHEN WILL WE BEGIN TO REDUCE ALPHA AND BETA ERRORS IN STATISTICAL PSI EXPERIMENTS?

Ulrich Timm (Institut für Grenzgebiete der Psychologie und Psychohygiene, Eichhalde 12, 7800 Freiburg i.Br., West Germany)

In many psi experiments some statistical selection errors are made, after whose correction the initial statistical significance disappears. These are Type I errors, more simply called alpha errors. That does not necessarily mean, however, that in these experiments real psi effects do not exist, since the usual methods, if utilized correctly, are often so ineffective--with regard to the rareness, instability, and inconsistency of psi effects--that they can only seldom lead to statistical significance. This inefficiency of statistical methods creates Type II errors, or beta errors. Therefore, our objective should not only be the reduction of alpha errors and the related decrease of spurious significances but also the reduction of beta errors and the related increase of real significance.

First I give an overview of those alpha errors that I call statistical selection errors. These show, simply stated, the following three qualities (Timm, ZP, 1983, 195-229):

(1) From a set of statistical results a single result is selected and evaluated by some significance test.

(2) The selection is not performed randomly but according to a criterion that is related to the level of the single result in that it directly or indirectly favors positive results.

(3) Despite this success-dependent selection, the significance test is carried out and interpreted in the usual manner without any correction.

*Chaired by Martin U. Johnson.