Homology, Analogy and Cybernetics ideas could help the counter-terrorism effort

Honorary Chair Prof. (Dr.) Daniel HOWARD
National Taipei University of Technology, Taipei, Republic of China (Taiwan)
Director, Howard Science Limited, UK
Fellow UK MOD's Defence Evaluation and Research Agency (DERA/QinetiQ), 2002-
dr.daniel.howard@gmail.com
dr. Adrian BREZULIANU
Greensoft SRL, Romania
Faculty of Electronics, Telecommunication and Information Technology,
"Gheorghe Asachi" Technical University of Iasi, Romania
adi.brezulianu@greensoft.com.ro

Abstract

Much of the success in law enforcement can be attributed to data gathering and its analysis. While many a plot has been foiled by detective work using clues gathered from observations, some of the elements of this detective work can be formalized from concepts that are commonplace in Biology and in Darwin's theory of evolution. We establish these connections to Biology and introduce the reader to another principle that arose in the old Cybernetics movement, arguing their applicability to criminology, and clarifying the ideas so as to guide research in this fruitful area that might benefit crime prevention theory and practice.

The nature of terrorism and counter-terrorism

The struggle between a terrorist attack and its counter-terrorist defenses reminds us of an example from Nature. It is the co-evolution between changes to the long bill in the oystercatcher and the flexible ligament that joins the left to the right valve in the bivalve mollusc (see Figure 1). To win its lunch, the oystercatcher must only marginally improve upon its bill overcoming a much bigger evolutionary improvement in the ligament of the mollusk.

Figure 1 – Oystercatcher opening a bivalve mollusk

The terrorist attack is like an oyster catcher's bill and its counter-terrorist defence is like the ligament of the bivalve mollusc! While a terrorist can manufacture an IED using widely available technology, it requires an enormous amount of effort, thinking, and advanced technology to design a personnel carrier capable of ensuring personnel safety against an IED explosion. Insurgents can use existing and commonplace technology: mobile phone, Internet, homemade explosives, but the defensive technology of counter-terrorism is necessarily orders of magnitude more involved and it is often leading edge technology. The defence, however, rarely stops the attack and then it often fails to sufficiently mitigate its effects. It remains extremely difficult and costly to defend against bombing campaigns, orchestrated hit and run militia activities, misinformation campaigns, and cyber attacks. At best, we can try to contain these attacks and decrease their frequency.

The value of Intelligence Analysis

Faced with this less than favourable situation, counter-terrorism activity has historically relied on the chance, induced, or coerced betrayal of the criminal organization either by its members, or by individuals in the adversary's immediate social network. Beyond tools such as the spreading of misinformation, efforts have focused on the infiltration of the criminal element by spies and undercover personnel. Through surveillance, and its reliance on the reports of informers and of the general public, counter-terrorism has been able to second guess a criminal organization to disrupt it, preventing it or delaying its operation. The value of infiltration has been to observe and to report but also to deliver advice and even to influence the conduct of the adversary from within.

Infiltration can not only be difficult, slow, and risky but sometimes impractical. For this reason, monitoring an adversary's activity over time, and the determination of patterns gathered from this activity, as input to the intelligence picture, arguably is a slow but extremely important tool of law enforcement. Such detective work holds patterns in a dual role. Patterns stimulate the construction of new theories but patterns also help to eliminate

some of the competing theories. The process of Intelligence Analysis is an active construction, an intellectual exercise which is grounded in evidence, and evidence has both a linear and a non-linear character. In a linear presentation, the frequency of a pattern and its addition to the body of evidence results in incremental progress. In a non-linear presentation, the single occurrence of a pattern may take on a defining significance.

For completion, and so as to prevent this paper from delivering an overly simplistic message, it is worth mentioning that there will always come to be instances when the availability of intelligence is judged to be detrimental. Consider the path of the Japan-US War during the Second World War. It is the considered opinion of some that the gathering and interpretation of intelligence had a detrimental effect, and that the Pacific War might have been delayed or even avoided [1]. We cannot consider in this brief paper the important psychological realities of the handling of information by the Intelligence Analysis: e.g. "warrior versus worrier" personality mix; dopamine levels; personality rivalries; and modus operandi such as "brawn versus brain", all can influence both the development and the quality of the intelligence picture [2].

The applicability of principles and laws gathered from interdisciplinary study

It is our view that the Intelligence Analysis will benefit from a number of ideas emanating from other fields. In this section, we tread upon a few of them to motivate interested readers to explore their connection to counter-terrorism.

Consider the "old cybernetics movement" that developed during the period 1950s-1970s. During the 1960s the British specialist in cybernetics W. Ross Ashby popularized a particular concept he called "the principle of requisite variety" (page 206 of [3]). Its motto is: "only variety can destroy variety". What does this mean? In layman terms, and for the benefit of our discussion, it is about attacks and responses to attacks. Every living creature has within its makeup a great number of in-built responses to a great number of possible attacks. Indeed, the power of imagination and problem solving of the human brain (and of the brains of other highly intelligent creatures) evolved to conjure up new responses to novel attacks. However, there will always be a certain type of attack for which there is no possible response: these attacks take the creature beyond the limits of its viability. For example, if the oxygen were to be taken out of the hermetic box, and nobody were to be around to respond to cries, then the creature that is trapped within the box would perish. As it has no response able to meet this attack, its viability would be compromised. This principle is apparent in many daily activities

including sport. Should two highly skilled football players meet on the pitch then the public would only see a minority of behaviours from the arsenal of their "attack and response" libraries. Indeed, we often see certain random moves with legs stepping over the ball because such "attacks" cannot by definition elicit a learned, and therefore a competent, response by the opponent.

Why do we suggest the Principle of Requisite Variety as useful to the counter-terrorism theory and practice? It is because it should assist both modelling and simulation. A further hypothetical example may illustrate this view. Imagine a nuclear disaster the size of Chernobyl with a very low background radiation in the area persisting for the following decades. It would be surprising to measure the incidence of cancer in the wild creatures that inhabit this area since the time of the accident as lower than normal! However, this counterintuitive notion is unsurprising if accounting for the Principle of Requisite Variety, but why? The principle leads us to reason that there must have been a time, millions of years ago, when a consistently and slightly higher level of radiation prevailed on this Earth. At such a time, Life might have evolved a defence mechanism against this persistent low level of radiation. This defence in the form of a chemical pathway might offer increased immunity against cancer. Such a theory is not implausible in light of the principle. In this hypothetical example, the investigator might use the principle to reason that the creature still has within it, such a fortunate response, and that the new environmental conditions might have triggered its genetic expression.

It suggests a technique. When modelling the dynamics of terrorist and counter-terrorist it is necessary to brainstorm and explore possible disruptive attacks and countermeasures of the criminal element. For some of these attacks it might be assumed that the criminal element possesses a response. Thus, sometimes *Gedankenexperiments* are sufficient instead of costly and risky validation through observation and experimentation, or instead of validation from painstaking data mining. Perhaps many attack-response pairs can be assumed to exist in this way owing to the Principle of Requisite Variety. This approach may attract criticism particularly with Reductionists but the approach is reasonable because, although it is important to collect data, it is arguably equally important to make reasonable assumptions guided by the principle.

Another principle that may be useful to Intelligence Analysis is to be found in Nature and also in Literature: "*Human nature is above all things—lazy. Every one confesses in the abstract that exertion which brings out all the powers of body and mind is the best thing for us all; but practically most people do all they can to get rid of it, and as a general rule nobody does much more than circumstances drive him to do.*" [4]. Consider the recent modelling efforts to combat drug crime in Amsterdam [5]. Although the

police constructed a social network which suggested to them how to disrupt organized crime, the disruption by police resulted in a more resilient drug network! This surprising and some may say paradoxical outcome, was probably because the original drug criminal network organization abided by the aforementioned principle of "laziness". It was organized in a less than efficient manner, and upon attack, it readjusted itself more effectively to defeat the police's interventions and attempts at its disruption [6].

Arguably, the hard sciences are not alone in establishing universal or quasi-universal principles. The Social Sciences have recently delivered a quasi-universal principle worthy of note: the "Youth Bulge Theory" [7]. It explains the conditions that lead to war, terrorism, general unrest and unstable government. For the benefit of this discussion, what can we take from the study of such a principle? Surely, it is important to understand both the causes that make a principle relevant, and to study the exceptions to the universality of a principle. Take the former for the "youth bulge": arguably its seed is the lack of education of women because if women finish some level of education then the number of children per mother drops dramatically, thus preventing the "youth bulge". What about the exceptions to universality? It becomes productive to studying rare cases that represent exceptions to the rule by means of comparisons, e.g., why did country x collapse into violent unrest and war whereas country y did not. We suggest that comparative exercises in the applicability of principles are most informative.

An important principle from Nature: Homology vs. Analogy

Further we propose that the intelligence community pay increased attention to yet another important principle from Nature. It is submitted that it is useful to learn to recognize the difference between a Homology and an Analogy in the Intelligence data.

It was Konrad Lorenz who in his 1973 Nobel Lecture [8] at the Karolinska Hospital in Stockholm first popularized the idea that the concept of homology also applies to culture and to technology. He illustrated this idea in a number of figures. We have reproduced his figure 5 as Figure 2 to illustrate this idea that depicts the evolution of train carriages. Even after the more technologically efficient concept of a central corridor was developed, many trains continued to be designed to resemble the old horse-drawn coach!

Similarly, the habits of a terrorist or criminal are inherited by his or her apprentice. As a trivial example of this, consider the design of a certain instrument of terror (IED, explosive package, misinformation campaign, computer virus, etc.). If it were possible to analyze its design, one would see within it solutions that are inherited (homology) and others which are re-discovered (analogy). To differentiate one from the other is to learn how to use homology to identify the criminal organization and its makeup.

Homologies can be easy to identify. For example, a certain design has something unnecessary and for no good reason, or it makes an arbitrary choice in the position of an item that could go anywhere, at no detriment to functionality. In such cases, such small details represent huge insights as to individual criminals and the nature of their association. The Intelligence Analyst must be trained to pay attention to such small details.

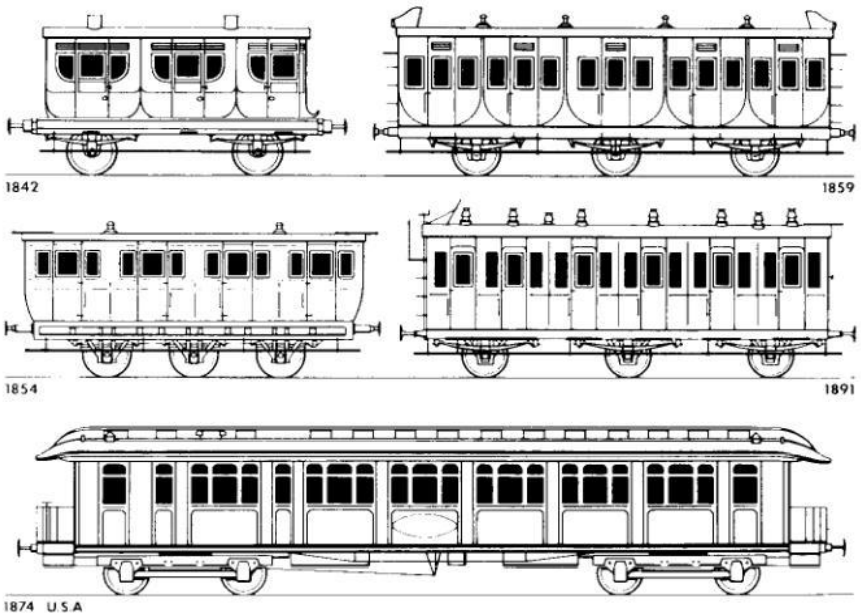

Figure 2 – Reproduced from Konrad Lorenz Nobel Lecture, 1973. It is an example of homology in technology that characters traceable to the ancestor, the horse-drawn coach should persist against the interests of technical progress in railway carriages.

Other times, however, the homologies are hard to discern. In contrast to a homology, an analogy is a principle that is independently rediscovered. For example, consider the re-discovery of flight in Nature by birds, bats, and insects. It is hard sometimes to learn to differentiate between a homology and an analogy. Here is something that would require a different type of training.

The application of homology to the natural sciences is as active today as in the past. In chemistry it is applied very successfully to the problem of protein folding and to the evolution of protein families [9]. Homology finds application in scientific fields beyond the sub-fields of Cladistics and Phylogenetics as it remains a popular concept in Astrophysics by shedding light on the seed of the structures in the Universe that we observe today.

Conclusions

Our proposal to the Intelligence Analysis community is to research how scientists have learned to differentiate an analogy from a homology in Nature. Learning this skill will enable the Intelligence Analyst to better grapple with the complexity that is inherent in detective work, with the ultimate objective of achieving timely and less ambiguous decision making.

We have also proposed familiarization with, and use of, some of the concepts that arose in the fruitful period of research between 1950^{s}-1970^{s} in the "old cybernetics" movement. The gain here is to use the principles to work with confidence to arrive at more complete models. Such concepts may help to deliver more reliable simulation models of criminal networks.

Top down models have been used to manage the under-determination that typifies detective work[i] and the Intelligence Analysis therefore has most probably adopted some of these concepts informally. However, a formal connection to Cybernetics and Biological ideas has not to our knowledge been made, nor has it been explored in the context of counter-terrorism.

Interdisciplinary study is an effective method to achieve innovation and invention. For this reason, it is submitted that Intelligence Analysis should explore all possible connections with established concepts from many other fields. Such efforts may deliver worthy contributions to its theory and practice.

References

[1] Battle Over Intelligence: the Path of the Japan-US War, NHK Documentary, 1st March, 2014, NHK World, NHK Broadcasting Corporation, Japan.

[2] Brain Games, Series 2, Episode 7. Distributor: National Geographic Channel (2011-), USA.

[3] W. Ross Ashby. An Introduction to Cybernetics. Chapman and Hall Ltd and University Paperbacks, Methusen and Co., 1964, (Reprinted 1970, SBN 412 05670 4 4.3).

[4] Harriet Beecher Stowe. In chapter 6 of "Household Papers and Stories", Boston and New York. Houghton, Mifflin and Company. The Riverside Press, Cambridge 1896. (first edition 1864).

[5] Paul A. C. Duijn, Victor Kashirin, Peter M. A. Sloot. "The Relative Ineffectiveness of Criminal Network Disruption", Nature Scientific Reports 4, Article number: 4238, 28 February 2014. doi:10.1038/srep04238

[6] Conclusion reached in discussion between Daniel Howard and Peter Sloot at the SimCity symposium at the Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO), Saint Petersburg, September 2013.

[7] Gunnar Heinsohn: Finis Germaniae? Die Zeit, KURSBUCH 162. Abgerufen am 8. Juni 2009.

[8] Konrad Lorenz, "Analogy as a Source of Knowledge", Nobel Prize Lecture, Physiology and Medicine, Karolinska Hospital, Sweden, December 12, 1973.

[9] In-Geol Choi and Sung-Hou Kim, "Evolution of protein structural classes and protein sequence families", PNAS, vol 103, no. 38, 14056-14061, Sep 19, 2006.

[10] C Baber, N A Stanton, D Howard and R J Houghton. "Predicting the structure of covert networks using genetic programming, cognitive work analysis and social network analysis" In: NATO Modelling and Simulation Group (NMSG) Annual Conference, Brussels, Belgium, 2009.

Adrian Brezulianu has a Ph.D. degree in Artificial Intelligence / Medical Electronics from Technical University of Iasi, Romania. He is Managing Director at Greensoft SRL Company during the last 10 years and as Professor at Faculty of Electronics and Telecommunications, Iasi, Romania during the last 20 years. He gained experience on running significant software projects for corporate entities on the area of utilities (Electrica Romania, CEZ Romania, CEZ Albania, Water companies, Oil companies etc…), specific ESRI GIS applications (telecom, electricity, cadaster etc..) and also on developing artificial intelligence solution on the area of industrial optimization, supply chain management, employees scheduling and profiling. He is author of 8 books, 15 journal articles and over 30 conference article. He also won 4 research projects as grant director in the area of signal processing, optimization and scheduling.

Daniel Howard has BS MS and PhD degrees in Chemical Engineering and Computational Mechanics. He is a former Rolls-Royce Research Fellow of the Numerical Analysis group of University of Oxford. From 1996-2009 he worked at the UK Defence Research Agency where he was promoted to QinetiQ Fellow in 2002 as the agency became QinetiQ. For one of his publications he has received an accolade from the UK Journal of Defence Science. Since 2006, he started Howard Science Limited, a UK SME that has won mathematical and data modelling research contracts which, together with UK Human Factors professors has participated in unclassified research project work for the UK Counter Terrorism Theory Centre. Previously, the team won an MOD Competition of Ideas. He is currently the Honorary International Chair Professor at the National Taipei University of Technology.

[i] Important and practical past and present field work has succeeded by such means to thwart terrorism. Reference [10] is a recent presentation of a theoretical example that illustrates use of a top down model to manage the under-determination of theories that can arise from surveillance data: although this illustrative example may be a touch over prescriptive.