Breaking bad systems: using work domain analysis to identify strategies for disrupting terrorist cells

Paul M. Salmon, Tony Carden & Nicholas J. Stevens

Centre for Human Factors and Sociotechnical Systems, University of the Sunshine Coast, Australia

ABSTRACT

Terrorism represents a major global issue. Despite decades of research, interventions designed to prevent or disrupt terrorist activities are failing to adequately control the problem. This paper argues that a human factors systems-thinking approach may support the identification of novel, holistic and impactful interventions. To demonstrate, a systems analysis of a generic Islamic State terrorist cell, created using the work domain analysis phase of cognitive work analysis, is presented. The analysis is subsequently used to identify opportunities for disrupting terrorist cells and their activities. In addition to well-known and already applied interventions, the analysis identified a series of other opportunities for disrupting terrorist cell activities. Examples discussed include strategies designed to disrupt propaganda activities and the planning of terrorist attacks. The analysis also showcases the potential use of systems ergonomics for disrupting, as well as optimising, sociotechnical systems. The implications for ergonomics generally as well as counter-terrorism activities are discussed.

KEYWORDS

Terrorism, human factors, systems thinking, work domain analysis

Introduction

Recent events worldwide demonstrate clearly that the threat of terrorism is both escalating and evolving. Since 1970 well over 380,000 people, including both victims and perpetrators, have been killed worldwide because of terrorist attacks (START, 2016). In the UK alone, since 2000 over 120 people have been killed and scores injured (START, 2016). Notably, the nature of terrorist attacks has not been homogenous (Schiermeier, 2015), ranging from hijackings, mass shootings and stabbings, to car and suicide bombings, attacks on critical infrastructure and more recently the use of vehicles as weapons in ramming attacks. Whilst a significant amount of resources is expended on counter-terrorism activities, the agility, breadth and reach of terrorist groups is such that it is becoming increasingly difficult to prevent new and emergent forms of attack. Although much effort has been undertaken in investigating, developing and implementing counter-terrorism strategies, it is widely acknowledged that new thinking is required (e.g. Navarro & Villaverde, 2014).

This paper argues that the discipline of ergonomics can play a key role in counter-terrorism and that systems ergonomics approaches offer a useful framework to support the development of strategies designed to prevent terrorist attacks. Systems thinking refers to a philosophy currently prevalent within the discipline of human factors and ergonomics. It is most prominent in accident analysis and prevention and is characterised by a series of accident causation models and analysis methods (e.g. Leveson, 2004; Rasmussen, 1997). Contemporary models are underpinned by the notion that safety and accidents are emergent properties arising from non-linear interactions between multiple

components across complex sociotechnical systems (e.g. Leveson, 2004). A key tenet is that adverse behaviours emerge from the interactions between components across entire work systems. Therefore, countermeasures should be holistic and introduced across all aspects of the system in question. This is in juxtaposition with the traditional reductionist approach of attempting to fix components in isolation. Accordingly, a range of systems ergonomics methods exist that support the analysis and design of sociotechnical systems (Salmon et al., 2017).

These methods provide the capability to describe entire systems, their component parts, and importantly the relationships and interactions between these parts. Whilst the detailed and rich outputs are typically used to support the optimisation of systems, it is precisely these features that provide a capacity to also inform the disruption of systems. This represents a new endeavour for our discipline that potentially opens up other areas in which ergonomics can be used to disrupt systems that are designed specifically to achieve illicit outcomes e.g. child sex abuse, the dark net.

The aim of this paper is to demonstrate how a systems ergonomics approach can be used to support development of strategies designed to disrupt terrorist cells in 'infidel' cities. This is achieved through presenting the findings from an initial exploratory study in which Work Domain Analysis (WDA), the first phase of Cognitive Work Analysis (CWA; Vicente, 1999), was used to develop a model of an Islamic State (IS) style terrorist cell. In turn, the WDA model was used to support the identification of strategies that could be used to disrupt the cell and its activities. The analysis forms part of a broader research program exploring the use of systems ergonomics in counter-terrorism.

Cognitive Work Analysis

CWA (Vicente, 1999) is a systems analysis and design framework that has previously been used both to analyse complex sociotechnical systems and to inform system design or redesign activities (See Stanton et al., 2017). Important features of the framework are that it focuses on identifying the constraints imposed on behaviour and that it can be used in a formative capacity to identify ways in which behaviour could occur. The framework has been used extensively in design to support the optimisation of sociotechnical systems (Read et al., 2017). As a result of the focus on constraints, design recommendations often involve making constraints more explicit to users, removing or adding new constraints, or better exploiting existing constraints to support behaviour (Stanton et al, 2013). In the present research program, CWA was selected as it can be used to identify new constraints on the behaviour of terrorist cells or ways in which to strengthen the existing constraints under which they operate.

The framework comprises five analysis phases (Vicente, 1999). In the present study the first phase, Work Domain Analysis (WDA) was used. WDA is used to provide an event and actor independent description of the system under analysis: in this case an Islamic State (IS) style terrorist cell 'system'. The aim is to describe the purposes of the system and the constraints imposed on the actions of any actor performing activities within that system (Vicente, 1999). This is achieved by describing systems at the following five conceptual levels using the abstraction hierarchy method:

1. Functional purpose: The overall purposes of the terrorist cell and the external constraints imposed on its operation;
2. Values and priority measures: The criteria that the terrorist cell and those associated with it use for measuring progress towards the functional purposes;
3. Generalised functions: The general functions that are necessary for the terrorist cell to achieve its functional purposes;
4. Physical functions: The functional capabilities and limitations of the objects within the terrorist cell system that enable the generalised functions; and
5. Physical objects: The physical objects within the terrorist cell system that are used to undertake the generalised functions.

The output is a detailed description of the system under analysis in terms of the constraints influencing behaviour and the physical objects (and their affordances) and functions that enable the system to achieve its functional purpose. Importantly, the abstraction hierarchy model uses means-ends relationships to link nodes across the five levels of abstraction. In the present analysis this provides the capability to determine how removal or disruption of nodes impacts the terrorist cell's overall functional purpose.

Method

Three analysts with significant experience in applying CWA and specifically WDA in a range of domains (e.g. defence, road and rail transport, land use and urban planning, off-road driving, outdoor education) were involved in conducting the analysis. The process involved two analysts drafting an initial abstraction hierarchy for a generic terrorist cell based on publicly available information such as websites, news reports and the research literature. Following this, the draft analysis was given to a third analyst who reviewed and refined the draft based on a review of relevant documentation including academic literature (e.g. Cook, 2009), journalistic commentary (e.g. Wood, 2016) and publicly available jihadi writings. Once the third analyst had completed the second refined draft version all three analysts held a day workshop in which they worked through the abstraction hierarchy and revised the model until all agreed on its content.

Once the abstraction hierarchy was finalised a process of 'node breaking' was initiated whereby the analysts systematically broke each of the nodes from the bottom three levels of the abstraction hierarchy. This involved taking each individual node, breaking the node, and determining the resulting impacts on the terrorist cell's values and priorities and functional purposes. For example, for the purpose-related function 'Propaganda' the analysts identified that, should this function not be achieved, the functional purpose of 'Create fear' would be negatively impacted as well as various values and priorities such as 'Exposure', 'Membership of IS', 'Vilification and division', 'Uncertainty', 'Disruption', 'Cell capacity' and 'Number of converts'.

For each broken node that was deemed to have an adverse impact on the terrorist cell's functioning, the analysts then brainstormed ways in which the node could forcibly be broken through counter-terrorism strategies. Nodes linked underneath each broken node via means-ends links were used to support this process by examining what nodes were required to achieve the broken node. For example, for the purpose-related function 'Propaganda', the object related process 'Communication' and related physical objects such as 'Internet' and 'Social media platforms' were considered when identifying strategies designed to disrupt propaganda activities.

Results

The terrorist cell abstraction hierarchy is presented in Figure 1. A specific example of the broken nodes analysis surrounding the purpose-related function 'Propaganda' is overlaid on the abstraction hierarchy. An extract of the broken nodes analysis outputs is presented in Table 1.

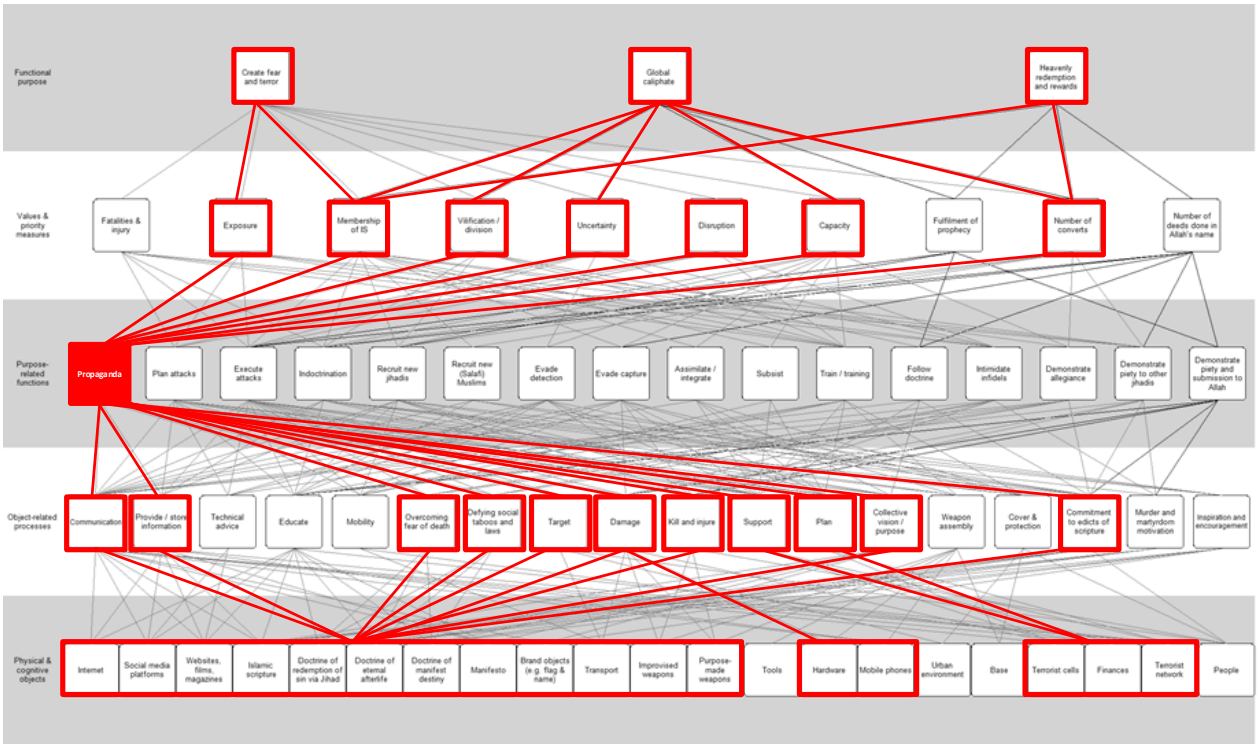

Figure 1. Terrorist cell abstraction hierarchy. Bold lines show the nodes and links disrupted when propaganda activities are targeted

While all system elements shown at the four lower levels of the abstraction hierarchy contribute to the achievement of system purposes, some appear to be both more critical to that achievement and more inimical to people in the broader society. For example, certain objects have multiple affordances, suggesting that they may be key objects to target in disruption activities. For example, objects such as the internet and social media have multiple affordances including ‘communication’, ‘store and communicate information’, ‘technical advice’, and ‘education’. Likewise, certain purpose-related functions are required to achieve multiple values and priorities. For example, ‘Propaganda’ supports the attainment of various values and priorities, including ‘Exposure’, ‘Membership of IS’, ‘Vilification and division’, ‘Uncertainty’, ‘Disruption’, ‘Cell capacity’ and ‘Number of converts’.

It can also be seen that function dependence varies among processes and objects. For example, ‘Improvised weapons’ and ‘Purpose-made weapons’ represent a useful functional redundancy: if one is absent, the other will support the process ‘Kill and injure’ just as effectively. In contrast, although each of the object-related processes it supports are also supported by other objects, the cognitive object ‘Doctrine of eternal afterlife’ is unique. This uniqueness offers a focus for disruption efforts. If redundant system elements are disrupted, alternative elements can still support higher level elements. If unique elements are disrupted, there can be some confidence that the system will be degraded.

A final interesting aspect of the abstraction hierarchy is the presence of cognitive objects as well as physical objects at the physical objects level. Cognitive objects are characterised as canonical ideas which constrain behaviour in a similar manner as physical objects. Like the physical objects in the functional structure of a system, cognitive objects are highly incorrigible. In the present analysis several of the objects could be considered more cognitive than physical in nature. These include ‘Islamic scripture’, the ‘doctrine of redemption of sin via jihad’ (e.g. Quran 4:74), the ‘doctrine of eternal afterlife’ (e.g. Quran 30:40), the ‘doctrine of manifest destiny’ (e.g. Quran 8:39), and ‘manifesto’.

Breaking nodes

To demonstrate the node breaking analysis the purpose-related functions 'Propaganda' and 'Plan attacks' are focussed upon. The 'Propaganda' function supports the attainment of various values and priorities, including 'Exposure', 'Membership of IS', 'Vilification and division', 'Uncertainty', 'Disruption', 'Cell capacity', and 'Number of converts'. These values in turn support all three functional purposes 'Create fear and terror', 'Global caliphate', and 'Heavenly redemption and rewards'. Disrupting the propaganda function is therefore likely to have a significant impact on the terrorist cell's activities and indeed their attainment of their functional purposes. As shown in Figure 1, the propaganda function is supported by 17 objects ranging from the internet and social media, scripture, doctrine and manifesto to finances and other terrorist cells. This suggests there are various opportunities to disrupt propaganda activities. These include disinformation campaigns, monitoring and restricting the use of the internet and social media, and directly removing sources of propaganda.

The nine processes identified supporting the function 'Plan attacks' were found to be afforded by seventeen physical objects. The object-related process 'Communication' appears to play a key role in planning and is afforded by objects that support the flow of inspirational, educational, technical and strategic information to terrorist cells or individuals who are planning attacks in 'infidel' cities. These objects include 'Internet', 'Social media platforms', 'Websites, films and magazines', and 'Terrorist network'. While preventing unknown plotters from accessing the internet seems unfeasible, work to disrupt or degrade this information flow (e.g. Twitter PublicPolicy, 2017) appears, on the basis of this analysis, likely to disrupt performance of the terrorist system. Strategies identified to achieve this included directly restricting sources of communication (e.g. shutting down websites), introduction restrictions around communication via social media (e.g. WhatsApp) and removing or corrupting communication materials.

Table 1: Extract of broken node analysis.

Broken node	**Functional purposes and values and priorities adversely impacted**	**Example strategies designed to break node**
Purpose-related function Propaganda	*Functional purposes* Create fear and terror, Global Caliphate, Heavenly redemption and rewards *Values and priorities* Exposure, Membership of IS, Vilification and division, Uncertainty, Disruption, Cell capacity, Number of converts	1. Counter-propaganda/Disinformation campaign conveying alternative/confusing messages around collective vision and commitment to scripture. 2. Create new leadership persona designed to create uncertainty. 3. Disrupt sources of education e.g. social media. 4. Mount multifaceted counter-propaganda campaign via social media. 5. Directly restrict propaganda sources e.g. shutting down websites. 6. Restrictions around use of social media platforms e.g. WhatsApp. 7. Compromise publishers of propaganda materials. 8. Removal/Corruption of on-line propaganda materials.
Purpose-related function Plan attacks	*Functional purposes* Create fear and terror, Global Caliphate *Values and priorities*	1. Monitor planning activities (e.g. WhatsApp, mobile phones, email) 2. Minimise targets and opportunities to attack - removing known vulnerabilities

	Fatalities and injury, Exposure, Uncertainty, Disruption	3. Proactive identification of new and emergent targets along with appropriate counter-terrorism strategies 4. Monitor acquisition of products known to be used in attacks 5. Use big data analytics to identify groups engaged in planning 6. Better coordinate restriction of targets and removal of vulnerabilities 7. Consider potential terrorist attacks when designing known targets e.g. cities, airports, vehicles, road networks 8. Disrupt the ability to acquire or construct weapons.

Discussion

Both terrorism and counter-terrorism take place within complex dynamic sociotechnical systems. An important advantage of systems ergonomics methods is that they support the description and analysis of overall systems including the interconnectedness of their parts. This allows analysts and policy makers to predict whether various system elements and strategies may complement or impede each other. The aim of this paper was to demonstrate how a systems ergonomics approach can be used to support development of strategies designed to disrupt terrorist cells operating in 'infidel' cities. This was achieved through developing an abstraction hierarchy model of a generic IS style terrorist cell, which in turn was used to support the identification of strategies to disrupt the cell and its activities.

An important initial finding is confirmation of the ability of systems ergonomics methods to identify ways in which to disrupt system performance, in addition to their well-known capacity for identifying ways to optimise systems and enhance human wellbeing (IEA, 2000). In the current application the analysis was used to identify ways to disrupt the performance of a system that is inimical to human wellbeing. This indicates that there are other areas in which systems ergonomics can be used to disrupt systems that have either been designed specifically to support illicit behaviours or are unintentionally creating adverse outcomes. Potential application areas for systems ergonomics therefore include child sex abuse, the production and trade of illicit drugs, fraud, illegal activity in the dark net, climate change, and hunger and famine.

The analysis itself supported the identification of various potential counter-terrorism strategies designed to disrupt or 'break' critical terrorist cell functions, and the objects that they use to achieve these functions. For the examples presented around propaganda and planning of attacks, disruption strategies ranged from disinformation and counter propaganda campaigns, attempting to disrupt or remove sources of education and technical advice to the use of big data analytics to monitor communications and the acquisition of products and devices known to be used in terrorist attacks. Many of the strategies identified are currently being or have been deployed by governments, security and intelligence agencies, and corporations (e.g. Twitter, Facebook). For example, the UK Home Office recently announced the intention to modify laws in order to strengthen restrictions around the viewing of terrorist content online (Home Office, 2017). This is similar to some of the strategies identified when focussing on disruption of the propaganda and planning of attack functions.

The node breaking exercise did, however, reveal other interesting strategies. From the plan attack function one example is the proactive identification of new and emergent targets (i.e. before terrorists identify them) and subsequent modification to reduce their vulnerability. This appears particularly pertinent in known target areas such as cities, airports, and stadiums; however, it should also apply in areas not previously subjected to attacks. Another strategy was the consideration of terrorist attacks during the design of artefacts known to represent weapons and targets (e.g. vehicles, urban spaces). Whether any of the strategies identified could be deployed within the constraints of risk, cost and feasibility is an important question that warrants further research. In relation to propaganda the importance of disinformation was also highlighted with various strategies focussed on using disinformation to minimise the impact of propaganda, training and education materials. One interesting strategy here was the development of IS personas to undertake covert disinformation campaigns.

An additional implication of the analysis is that the impact of counter-terrorism strategies seems likely to be enhanced through better coordination during their design and implementation. Most of the strategies identified would require coordination between multiple agencies in order to be appropriate and effective. In addition, the model suggests that objects and functions should be considered together as opposed to components in isolation. This requirement for improved coordination therefore relates both to the strategies themselves but also to the groups developing and implementing them.

Finally, an interesting feature of the analysis was the presence of cognitive objects within the abstraction hierarchy. Whilst abstraction hierarchy analyses have traditionally only included physical objects, recent analyses undertaken by the authors suggest that the inclusion of cognitive objects is beneficial (e.g. Carden et al., 2017; McLean et al., 2017). In the present analysis there are a series of cognitive objects that seem to present opportunities for counter-terrorism. For example, the absence of belief in an afterlife seems highly likely to disable jihadis' capacity to overcome the fear of their own death and to defy social taboos and laws against killing innocents. This in turn would critically undermine the 'Execute attacks' function. While the disabling of these cognitive objects may present a structural leverage point, the feasibility of doing so presents challenges. Some or all of these doctrines extend well beyond jihadi belief. They are shared by non-jihadi 'quietist salafists' (Wood, 2016), mainstream Muslims, Christians, Jews, Hindus, many Buddhists and most other religions including new-age spiritual belief systems. This is what makes them canonical and is also what makes them such powerful objects within the terrorist system considered here. Strategies to disrupt them may provide effective new counter-terrorism measures.

As an exploratory study there are some limitations worth noting. The study was based only on publicly available data and did not involve interviews with subject matter experts (e.g. those currently working in counter-terrorism) or indeed terrorists. In addition, it should be acknowledged that there are many other non-Islam terrorist groups who could be studied. Future research should therefore explore the use of additional data sources (e.g. interviews, case study analyses) as well using other forms of terrorist group as the unit of analysis.

Conclusion

New approaches are required to combat the significant problem of terrorism. This paper demonstrated how systems ergonomics can potentially be used to understand terrorist cell systems and to identify counter-terrorism strategies. The application of WDA allowed a holistic view of the whole of the terror cell 'work system', which in turn enabled the identification of critical disruption points. Closer analysis of each of these points including the risks, costs and feasibility of disrupting them could potentially support an optimal, targeted strategy for disrupting terrorist cell systems. Further applications of systems ergonomics in this area are encouraged.

References

Callimachi, R. (2017, February 4). Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar. *The New York Times*. Retrieved from www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html

Carden, T., Read, G., Goode, N., Salmon, P. M. (2017). Sociotechnical systems as a framework for regulatory system design and evaluation: using work domain analysis to examine a new regulatory system. *Applied Ergonomics*, Accepted for publication December 2016

Cook, D. (2009). Islamism and Jihadism: The Transformation of Classical Notions of Jihad into an Ideology of Terrorism. *Totalitarian Movements & Political Religions, 10*(2), 177-187. doi:10.1080/14690760903119100

Home Office (2017). Law tightened to target terrorists' use of the internet, https://www.gov.uk/government/news/law-tightened-to-target-terrorists-use-of-the-internet, accessed 4th October 2017

IEA. (2000). The Discipline of Ergonomics. Retrieved from www.iea.cc

Leveson, N. G. (2004). A new accident model for engineering safer systems. *Safety Science*, 42:4, pp237-270

Mclean, S., Soloman, C., Gorman, A., Salmon, P. M. (2017). What's in a game? A systems approach to enhancing performance analysis in football. *Plos One*, 1-15

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database. Retrieved from www.start.umd.edu/gtd

Navarro, J. M. B., Villaverde, J. C. (2014). The future of counter-terrorism in Europe. The need to be lost in the correct direction. *European Journal of Futures Research*, 2:50, https://doi.org/10.1007/s40309-014-0050-9

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, 27:2/3, 183-213

Read., G. J. M., Beanland, V., Lenne, M. G., Stanton, N. A., Salmon, P. M. (2017). Integrating Human Factors methods and systems thinking for transport analysis and design. CRC Press, Boca Raton, FL

Salmon, P. M., Walker, G. H., Read, G. J. M., Goode, N. & Stanton, N. A. (2017). Fitting methods to paradigms: are ergonomics methods fit for systems thinking? *Ergonomics*, 60:2, 194-205.

Schiermeier, Q. (2015). Attempts to predict terrorist attacks hit limits Erratic human behaviour and incomplete information plague efforts to model risk. *Nature,* 517, 419–420

Stanton, N.A., Salmon, P.M., Walker, G.H. & Jenkins, D.P. (2017). Cognitive Work Analysis: Applications, extensions and future. CRC Press, Boca Raton, FL

Twitter PublicPolicy. (2017). Global Internet Forum to Counter Terrorism. Retrieved from https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html

Vicente, K. J. (1999). *Cognitive work analysis : toward safe, productive, and healthy computer-based work*. Mahwah, N.J. Lawrence Erlbaum Associates

Wood, G. (2016). *The Way of the Strangers, Encounters with the Islamic State*. U.K. Penguin