ASAC 2003
Halifax, Nova Scotia

Wm. David Salisbury
School of Business Administration
University of Dayton

Abhijit Gopal
Richard Ivey School of Business
University of Western Ontario

TALES FROM THE DARK SIDE: INTERNATIONAL CRIMINAL AND TERRORIST GROUPS AS KNOWLEDGE-BASED ORGANIZATIONS

With the stunning success of the last year's attacks on the United States and the continuing success of the international drug trafficking, it is clear that criminal and terrorist organizations have made effective use of a variety of available organizational forms and information technologies to advance their agendas. While their ends may be seen as contemptible, the means that they have adopted include an extremely high level of technical sophistication, and effective use of virtual and networked forms of organization. Using the lens offered by adaptive structuration theory, this article is intended to advance a research agenda that some may find useful in understanding how technologies that have enabled the dramatic growth of commerce around the world have also provided yet another opportunity for those who would appropriate them to nefarious ends. This article will provide some examples of what international terrorist and criminal groups have been able to accomplish by the skillful appropriation of virtual organizational forms and knowledge management concepts. Implications are discussed.

Introduction

The game of cricket is as decidedly a part of the globalization phenomenon as any form of multinational commerce. With the help of the Internet, cricket and its affairs are visible to global diasporas in an unprecedented variety of locations, giving people who had lost touch with that aspect of the community they once knew a means to bring it back into their lives. This visibility, however, has its dark side. As worldwide audiences prepare for the 2003 World Cup in South Africa, Zimbabwe, and Kenya, the latter two countries suddenly find themselves in danger of being removed as host nations due to the terrorist threat they are known to harbor; after all, such groups would clearly be tempted by an event of this magnitude as a means to engage an audience and thus advance their particular agendas.

Facilitating this new interconnectedness is the same infrastructure that powers the world of global commerce: the availability of open standards and a robust information infrastructure provided by the Internet (Barabasi, 2002; cf. Zanini and Edwards, 2001). Examples are TCP/IP, HTML, XML and various file format standards (e.g. Quicken .qfx, Acrobat .pdf, or graphic formats such as .jpg and .gif) that enable easy communication between enterprises of all stripes, their customers, their suppliers, their competitors, and the oversight organizations that monitor their activities. Indeed, new technologies enable law enforcement agencies to more effectively communicate critical information to police officers on the street; witness Public Safety Group's software "PocketCop©", provided to police officers on an HP iPAQ, with infrastructure and other hardware also provided by Hewlett-Packard (Hewlett-Packard Company, 2003). However, as with many well-intended technological innovations there are less favorable outcomes as well (cf. Tenner, 1997); some of the very elements (e.g. robust infrastructure and open standards) that make global commerce and better information more readily available to law enforcement also put in place the mechanisms which enable terrorists and criminals to be more effective in achieving their ends. In a world with open standards and a robust infrastructure, terrorist and criminal

organizations can attach to the infrastructure as easily as can those who would use it for "legitimate" ends; for example, what difference does it make to the network if the data packet is a legitimate bank deposit or a virus, or even monies being laundered by a terrorist organization?

It is true that the ready availability of a robust communication infrastructure has enabled the development of e-commerce, and has also enabled organizations to structure themselves in more of a networked form, with limited dependence on a hierarchy. However, a case can be made for the suggestion that the most effective practitioners of networked and virtual organizations have not been businesses or governments, but criminal and terror organizations. Some of these organizations have demonstrated extremely sophisticated capacity for understanding the advantages that can be gained by leveraging information and information technologies. Sophisticated data mining efforts are put in place by Colombian drug traffickers (Kaihla, 2002); equally sophisticated efforts at hiding messages using steganography have been engaged in by international terrorist groups such as al-Qaeda (Cohen, 2001; Ronfeldt and Arquilla, 2001).

Since even a cursory investigation of these groups reveals several examples of what some might see as a fairly sophisticated understanding of knowledge and its management, the present effort will endeavor to understand criminal and terrorist organizations as knowledge management systems. If we set aside, for the moment, our quite reasonable indignation at their goals and the means they use to achieve these, we discern patterns of use that provide their own clues about why these groups are so difficult to keep in check. We see innovative uses of information and communication technology that are often unmatched by the slow-moving institutions that set out to bring them to justice (cf. Castells, 1998). Our purpose in this paper is to initiate the task of looking carefully at a phenomenon from which we have, until now, averted our eyes. Let us make clear that we have no intention here of according any form of legitimacy to such groups and their uses of IT; we attempt merely, in a manner similar to Rayport's (2000) use of the concept of the 'viral' to point to how we might create more effective usage of information resources in organizations, to look at the kind of innovation that can emerge through the appropriation of technology in novel ways.

To achieve our purpose, we use a theoretical perspective well known in the information systems field which looks carefully at the manner in which IT is appropriated, adaptive structuration theory (AST), originally developed by DeSanctis and Poole (1994; cf. Poole and DeSanctis, 1992) to understand variable outcomes in the use of group support technologies. We briefly review AST next, and the suggestion that the schemata and resources it identifies, as well as its intellectual tradition, can be recast as knowledge and resources to store and transmit information and instructions among organizational members. We then examine several examples of how criminal and terrorist organizations have made effective use of existing technologies and technical infrastructures and how these uses are merely unanticipated extensions of what "legitimate" organizations have been attempting to do since the advent of the Internet as an information infrastructure to support business. Implications are discussed.

Adaptive Structuration Theory

Adaptive structuration theory (AST) is suggested as a means by which processes of technological appropriation in the workplace may be described. Originally developed by Poole and DeSanctis (1992) to address misunderstood findings in GSS research, AST suggests a novel theoretical path around theories that tend toward either highly individualistic or overly deterministic perspectives by invoking Giddens' notion of the "duality of structure" (DeSanctis

and Poole, 1994). Giddens indicates that structure is composed of both "rules" (normative constraints on action) and "resources" (social objects that enable interaction). From this perspective, structure is both imposed upon social action and emergent through interaction. While structures represented in technology can be seen as influencing its use, the technology itself, characterized by its structural potential, is influenced by participants' use of it; technologies are different to different users by virtue of their appropriation in a unique manner.

Several authors' efforts have acted as interpreters of Giddens by defining and clarifying the relationship between his primary concepts (e.g., Sewell, 1992; DeSanctis and Poole, 1994; Wheeler and Valacich, 1996; Salisbury and Stollak, 1999; Miller, Bartkowski and Salisbury, 2000). Further, empirical research on technological appropriation has revealed the fruitfulness of AST when compared with more voluntaristic or deterministic paradigms (Wheeler and Valacich, 1996; Chin, Gopal and Salisbury, 1997; Salisbury, Chin, Gopal and Newsted, 2002; Poole and DeSanctis, 1992). Indeed, this is a key advantage of structuration theory; it effectively avoids the pitfalls of voluntarism and determinism by conceiving of social structure as a "duality" that simultaneously constrains and enables social action (cf. Orlikowski, 1992; Sewell, 1992; Bordieu, 1998). Giddens conceptualizes this duality as "rules" and "resources", while Sewell suggests that the term "rules" is too abstract and vague to lend insight into social interaction (cf. Miller et al, 2000), instead defining the duality of structure as schemata and resources. *Schemata* are ideological frameworks that prescribe courses of appropriate action—in Sewell's terms, "recipes" for action. Further, Sewell (1992: 8) indicates that schemata are capable of being applied outside of the social sphere in which they were initially generated and internalized, a process he terms the "transposability of schemata." As an example, the rapid adoption of email can be said to have been largely a result of its metaphoric similarity to mailing a pen and paper letter; the idea of "mailing" a letter to an "address" was fairly easily transposed to its electronic equivalent.

However, the transposition of schemata does not necessarily suggest unreflective replications of interaction recipes across social situations. Sewell argues that the agency of social actors is found in their ability to use social recipes creatively to challenge the status quo or to meet the demands of novel situations. Following from the previous example, using an email attachment to transmit a computer virus to a target computer is substantively easier and has a greater chance of success (in that it can be made to look unsuspicious) than attaching infected code to programs and passing them using floppy disks. Since "snail" mail can often contain dangerous contents (e.g. explosives or anthrax spores), the idea of sending a virus through an email is a fairly natural extension of this logic.

Both Giddens and Sewell see *resources* as cultural products or objects that actors with access to them can enlist "to enhance or maintain power" (Sewell 1992: 9). Because resources are defined as meaningful within a particular cultural context, resource-rich actors are more capable of generating, disseminating, and legitimating schemata among group members. Specifically, Sewell identifies two different types of resources—namely, human and non-human resources—in explicating the process of resource-accumulation (cf. Fincham 1992).

Given recent writing on knowledge and knowing (Orlikowski, 2002), it is reasonable to assert that these "recipes for action", or schemata, are the know-how that members of an organization can put into practice as they engage the world. According to Sewell (1992), human resources are seen as products of schemata; a given number of soldiers (or police officers, or terrorists) will generate differing outcomes depending on conventions of engagement, strategies and tactics they represent, and the degree to which their training is actually enacted when called upon. As an example, Canadian troops tend to do better than many when placed in peace-keeping roles, perhaps because Canada sees this as a central purpose of its forces (Government of Canada,

2003) and trains them accordingly for this role. Inanimate resources cannot be seen directly as products of schemata, however; their utility when placed into action depends on schemata put in play as they are appropriated (Sewell, 1992); one person's box-cutter (or plastic comb; cf. *The Economist*, 2002) is another's deadly weapon.

The schemata called into play by terrorists reflect to a fair degree the cultural milieu from which they emerge. One of the key appeals of Osama bin Laden's message is to those who feel a sense of disenfranchisement with their own particular society (Rouleau, 2001). Religious terrorists, including some white supremacist groups in the United States (Vidal, 2002; Castells, 1998), tend to see themselves as a persecuted minority, victims of violence and/or oppression, and morally justified in any act they undertake against "infidels", "non-believers" or "mud people"; i.e. anybody who is not one of them (Hoffman, 1993). In the case of Colombian drug traffickers, the self-image is deeply based in their cultural identity, to the extent that Pablo Escobar, head of the Medellin cartel stated his preference for "… a tomb in Colombia (rather) than a prison in the United States" (Castells, 1998). Further, faced with limited resources (at least relative to the larger nation states such as the U.S.), these groups have historically demonstrated a penchant for creativity in appropriating various technologies to violent ends (cf. Arquilla and Ronfeldt, 2001).

Adopting the theoretical lens provided by AST and its intellectual tradition, our conceptualization of terror and criminal groups as knowledge-based organizations follows from this premise. We suggest that a central task of any knowledge-based organization is really one in which schemata are imbued in its membership through training, indoctrination and culture, and once the membership is dispersed to the field, to call these members into action consistent with their training, drawing upon human and non-human resources available to them. Resources that can be drawn upon in this context would include (but not be limited to) the robust information infrastructure provided by the Internet and other telecommunication networks. Before describing examples of how these have been appropriated, however, the relationship between knowledge and information technology is addressed.

Knowledge and Information Technology

When it comes to managing knowledge, there are two general classifications with which firms must cope. These are *explicit* knowledge and *tacit* knowledge (Polanyi, 1967). Explicit knowledge is *knowledge that is easily expressed;* it can be written down or passed verbally to others. Because of its ease in expression, explicit knowledge is more easily transferred and imitated. On the other hand, tacit knowledge is *knowledge that is difficult to articulate and express to others.* This nature of tacit knowledge is often discerned in the form of generally accepted background understandings (Garfinkel, 1964) about reality held by members of a culture or organization (cf. Berger and Luckmann, 1967, Goffman, 1974, Deal and Kennedy, 1982, Collins, 1992). Such knowledge emerges over time, and is learned by immersion rather than rote (Polanyi, 1967). Many times the possessor of the knowledge is unaware of its existence, due to its implicit nature. The management of this type of knowledge is a difficult process given that the knowledge is difficult to express. The knowledge may be expressed in terms of a restricted code (Bernstein, 1965) – a form of jargon – that, while obvious to organizational members may not at all be so to non-members. Indeed, members may not be consciously aware of the existence of the knowledge, and hence may be unable to communicate it to non-members (Bloodgood and Salisbury, 2001).

At its basic level, information technology can be seen as embodying two general capabilities with respect to knowledge; *codifying knowledge* and *creating networks* (cf. Hansen, Nohria and Tierney, 1999; Bloodgood and Salisbury, 2001). Knowledge may be codified into a decision support or expert system by making it explicit. For example, this is done in expert systems through the elicitation of knowledge from a domain expert by a knowledge engineer. Some knowledge has greater value when kept in a less explicit form (cf. Bloodgood and Salisbury, 2001). Consequently, another capability provided by IT for knowledge management involves not codifying the knowledge, but helping to keep track of persons with particular expertise, and enabling rapid communication between them. This type of approach to knowledge management enables the knowledge to remain tacit (cf. Bloodgood & Salisbury, 1998); by sending symbolic or encoded messages that have meanings to group members, but that would be less meaningful, even meaningless, to those outside the group (and hence without similar schemata to call upon to interpret the messages). Further, it also enables relatively rapid access by allowing people in the organization to easily identify who has knowledge and expertise relevant to their need and quickly contact them.

Terrorist and criminal groups have demonstrated effectiveness at both of these technology-enabled approaches to knowledge management. With respect to codified knowledge, terrorist groups use a variety of information technologies (e.g. the e-mail, CD's, websites) to provide instructional materials to their agents (cf. Arquilla and Ronfeldt, 1999). Colombian drug cartels have been especially effective in this effort, developing extensive knowledge management systems that are used to map movements of U.S. P-3 Orion surveillance aircraft by integrating pilot reports into detailed maps of radar coverage, and data mining systems that are used to track telephone calls of their membership, some of whom were killed when the system revealed telephone calls to government officials (cf. Kaihla, 2002).

With respect to building networks, terrorist groups have made noteworthy use of websites, chat rooms, list-servers and email to coordinate their efforts (Arquilla and Ronfeldt, 1999). Drug cartels have set up business to business exchanges for laundering money. The drug cartels efforts are enabled in part by sophisticated encryption systems bought off the shelf by front organizations, usually from U.S. companies (Kaihla, 2002), while many terrorist groups have also benefited from strong encryption, with one site advertising "…'CIA-proof' protection against electronic surveillance" (Arquilla, Ronfeldt and Zanini, 1999:67).

However, even when terrorists and criminals codify knowledge, it does not seem to be as rigid procedures for conducting operations, but for specific competencies that may be applied separately or in combination to meet a specific goal; e.g., members are given instructions on how to build a bomb, but not necessarily specific operational orders as to when and where to use it. In contrast, the nation-states that oppose these flexible, knowledge-based networks feature rigid procedures and clear division of labor that depends on the problems they face being divisible into clear-cut portions. One example of this is the rigid rules (usually bound by specific, detailed treaties) for cooperation between nation states; the ease of mobility around Europe since the advent of the EU has actually made it easier for criminal networks to operate there, exploiting jurisdictional gaps between the various nations and their police forces (cf. Castells, 1998).

Virtuality and Knowledge-Based Terror and Criminal Organizations

One upshot of the availability of robust infrastructure and open standards is the emergence of virtual organizational forms based on the sharing and enactment of knowledge (cf. Orlikowski, 2002). DeSanctis and Monge (1999:693) define a virtual organization as "a

collection of geographically distributed, functionally or culturally diverse entities that are linked by electronic forms of communication and rely on lateral, dynamic relationships for coordination." The nature of virtual organizations defined in this way means that they are rather malleable, with processes relationships, and structures among partners changing as shared goals and needs change. The malleability of virtual organizations means that they could be formed between partners for short periods to achieve specific, shared goals, and then just as rapidly disbanded. For example, groups that descended on the WTO talks in Seattle in 1999 (de Armond, 2001) represented a diverse agglomeration of labor, anti-globalization and environmental groups that, while they have some elements in common might also find themselves at cross-purposes on other issues.

With arguably one exception, criminal and terrorist organizations fit DeSanctis and Monge's definition of virtual organization. The one addition would be that there is some central organizing theme that binds at least the close-in members of the network together (cf. Ouchi, 1980; Maitland, Bryson and Van de Ven, 1986). In the case of al-Qaeda, for example, it has to do with establishing "a pan-Islamic Caliphate throughout the world by working with allied Islamic extremist groups to overthrow regimes it deems 'non-Islamic' and expelling Westerners and non-Muslims from Muslim countries" (Naval Postgraduate School, 2002). In most terrorist and criminal organizations, reciprocity and legitimate authority (such as one finds in a market or bureaucratic structure) are necessary, common values and beliefs are perhaps as important, if not more so. In terrorist groups, the legitimate authority is derived from the shared belief in the cause. In the case of Colombian drug cartels, legitimacy is rooted in their cultural identity (Castells, 1998; cf. Ronfeldt and Arquilla, 2001).

This particular understanding about the nature of terror and criminal groups is important, because these background understandings provide a shared interpretive context (cf. Zack, 1993) within which messages can be understood. This is also consistent with the idea of "tacit" knowledge (cf. Polanyi, 1967); tacit knowledge from our perspective is reflected in schemata that the group membership applies as they appropriate resources from their environment. This common frame of reference makes these groups capable of coordinating without a clear chain of command which could relatively easily be identified and disrupted, and communication using media that might be seen as extremely "lean" would be readily accomplished (cf. Lee, 1994). As a consequence, virtual organizational forms have been readily adopted and effectively used by terrorist and criminal organizations and further enable their knowledge management, communication and coordination efforts.

Indeed, in the presence of a strong base of tacit knowledge, or shared schemata, media that could be seen as extremely "lean" (Daft and Lengel, 1986) can be used to transmit messages that, while they would have no meaning to out-group members (cf. Bernstein, 1965), they would be very relevant to the membership – as we have even seen earlier during the development of the telegraph (Standage, 1998). Terrorist groups have been extremely effective in appropriating these to advance their agendas. Whether it is through fairly obvious means such as the website "maalemaljihad.com" (Higgins et al., 2002) or less obvious means such as coded messages sent via email and embedded in graphic images, various terrorist groups have found ways to get their message across, and coordinate their attacks across vast geographic distances. For example, al-Qaeda have been known to transmit messages to its membership through the use of steganography, literally "hidden writing" (Cohen, 2001); messages can be hidden in text or within graphics, or could even be hidden in plain sight on a website (e.g. a picture of a person with arms crossed). It would appear that terrorist networks have been extremely effective in terms of understanding tacit knowledge shared among themselves, and by the building of networks that leverage their tacit knowledge. Even if one looks to less technically sophisticated means of transmission (e.g. a speech given on TV), using common symbols and understandings within the

groups (or those who study them carefully), messages can be easily sent that, while they have very specific and explicit to the membership, would look like "squiggles" or "worms" to anybody else (Higgins, Leggett and Cullison, 2002).

Even the recruiting of new members is made easier for these groups by widespread availability of their message on Internet sites. Although the media in question are extremely lean and may not be the most useful for transmittal of anything like a "culture" (cf. Bloodgood and Salisbury, 1998), the sheer reach of the technical infrastructure means that by the law of averages individuals who share similar schemata – i.e. the sense of disenfranchisement and powerlessness as do those at the head of these organizations will be found. The wide reach of the Internet means that these candidate members will find the message, and some of them will likely respond. Those who do respond can be recruited to places where they can be trained and indoctrinated further, and then become "nodes" in the network that can be eventually activated to perform a particular task using lean, perhaps encoded, messages (cf. Gertz, 2002).

Even if not recruited and then deeply rooted in or near the core of the group, recruits with weaker ties to the core membership can still be useful. There is evidence to suggest the most important connections when it comes to accomplishing something that requires connections (e.g. getting a job; getting elements put in place to steal aircraft to demolish a building) are accomplished through so-called "weak" ties (Granovetter, 1973). For example, a social networking analysis performed by Valdis Krebs (reviewed in Stewart, 2001a) indicates that at least some of the hijackers on United 175 on 11 September were not closely tied to Mohammed Atta save that they were on the plane that day (having links with Atta described by Krebs as "more tenuous"), and indeed at least one of them apparently had no publicly known direct link with him prior to that day.

Taking this "weak ties" perspective to the extreme, even members with extremely tenuous links to the organization, but a belief in its message and a willingness to take action on its behalf can be outfitted and put into action. For example, some have advocated a "cyber-jihad", directed at Israeli government and business sites in particular, but also those of U.S., Indian, Australian and British interests as well (CNN, 2002). In response, Israel has appealed to its citizens to retaliate against Muslim, al-Qaeda and pro-PLO sites (Zanini and Edwards, 2001). Given the ready availability of hacking tools on the Internet, these "script kiddies" (users of such scripted hacking procedures) (Houle, 2002), whether or not linked to any particular terrorist group, are easily recruited and require no resources to be expended by the group for which they act. Further, such individuals can act independently of any specific group order, making the identification of any command and control structure difficult.

Indeed, terrorist groups have themselves been found vulnerable to these kinds of "hack attacks" as soon as they put up an Internet presence; the al-Qaeda website "al-Neda" (the Call), has in the past year been hacked by other groups redirecting the links to pornographic sites (Moaveni, 2002). It is unclear if this is the result of any U.S. sponsored group – actually it is reasonable to suggest the U.S. would like the site to stay up so its content could be monitored for tips as to the group's next move. Still, it does not require the U.S. to actively recruit anyone to undertake this; anyone angry at al-Qaeda and with access to the Internet could launch denial of service attacks, hack and deface their site, or engage any of a variety of other "cyber-attacks" (cf. Denning, 2001).

Discussion and Conclusions

Returning to our original premise, we believe that we have made it clear that the capabilities provided by a robust information infrastructure and open standards has enabled a variety of opportunities for those who would appropriate them to alternative ends, and we have described several examples of this phenomenon in action. By the application of their unique schemata in combination with the robust infrastructure and open standards embodied in the Internet, these groups have leveraged their resources to great effect. In contrast, nation-states have at times been caught flat-footed by the rapidity with which these groups can associate, accomplish their objective, and then disperse; consider the "swarming" attack described by Arquilla and Ronfeldt (2001). This has at times occurred despite less than perfect operational security; recall that critical messages were intercepted prior to 11 September, 2001, but the institutional understandings and procedures in place at the time simply did not allow these messages to be appropriately interpreted in time to avert those events.

In a world whose boundaries are defined to an ever-increasing extent not by national boundaries but by the inter-connectedness of its networks (Castells, 1996), the potential for terror and criminal groups to draw upon the robust infrastructure and open standards to advance their own agendas will likely increase (cf. Arquilla and Ronfeldt, 2001). We have asserted that the creativity of terror and criminal groups draws at least in part from their existence outside the mainstream of society, which enables them to cast off generally taken-for-granted understandings about "appropriate" uses of information technology and call it into use creatively for their purposes (cf. Arquilla and Ronfeldt, 2001; Castells, 1998; Kaihla, 2002).

Another contributing factor is that these groups have been aggressively pursued by various nation-states, and hence have been forced to evolve into flexible groups that do not confront their target institutions directly, but at their periphery, exploiting overlapping responsibilities and institutional rigidity, or by infiltrating the bureaucracy via bribery or extortion (Castells, 1998). The capacity provided by a robust information infrastructure and open standards enhances the ability to carry out such attacks. Indeed, the analysis of emerging terrorist groups by Arquilla and Ronfeldt (1999) indicates that a very deadly sort of natural selection is in play; as nation-states systematically surround and confront these groups, they have adopted by necessity the kinds of knowledge-based, virtual organizational forms to which businesses aspire.

We suggest that the examples provided here offer instruction in novel uses of information technology to enable knowledge-based virtual organizations that can be applied in a variety of domains, and hence several research avenues that may be pursued come to mind. One interesting avenue would be to investigate in depth the suggested relationship between disenfranchisement and innovative or unique appropriation of technologies. Another possible direction might be to investigate more carefully how nation-states can adopt the novel institutional changes suggested here and thereby resist this direct challenge to their sovereignty and legitimacy (cf. Castells, 1996; 1998). Further investigation as to what is "knowledge" and how it can be best "managed" is also indicated; clear understandings in this area would have the dual benefit of better understanding how criminal and terrorist groups operate, and also how nation-states can arrange their resources in a more effective manner.

The clearest implication that can be offered from this effort, however, is that simply engaging in technical solutions to address these issues merely leads to something of an arms race between "legitimate" and "illegitimate" uses of technologies, rather than lasting solutions to the underlying problems. The solutions here are not technical, but organizational and cultural.

References

Arquilla, J. and Ronfeldt, D. (2001). Afterword (September, 2001): The Sharpening Fight for the Future. In Arquilla, J. and Ronfeldt, D. (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. Santa Monica, CA: Rand, 363-371.

Arquilla, J., Ronfeldt, D., and Zanini, M. (1999). Networks, Netwar, and Information-Age Terrorism. In Lesser, I. O., Hoffman, B., Arquilla, J., Ronfeldt, D. F., Zanini, M., and Jenkins, B. M., Eds.), *Countering the New Terrorism.* Rand Paper MR-989-AF, 1999. Santa Monica, CA: RAND, 39-84.

Barabasi, A. (2002). Linked: The New Science of Networks. Cambridge, MA: Perseus Publishing.

Berger, P. L. and Luckmann, T. (1967). *The social construction of reality*. New York: Doubleday.

Bernstein, B. (1965). A socio-linguistic approach to social learning. In J. Gould (Ed.), *Penguin Survey of the Social Sciences 1965,* London: Penguin Books, 145-166.

Bordieu, P. (1998). *Outline for a theory of practice* (R. Nice, translator). Cambridge: Cambridge University Press (original work published 1978).

Bloodgood, J. M. and Salisbury, D. (2001). Understanding the influence of organizational change strategies on information technology and knowledge management strategies. *Decision Support Systems, 31*(1), 55-69.

Bloodgood, J. M. and Salisbury, W. D. (1998). What you don't know you know can hurt you: Considerations in using IT to transmit tacit knowledge in organizations. *Proceedings of the 1998 Association for Information Systems Americas Conference, Social Informatics and Information Systems Mini-Track*, Baltimore, MD, August 14-16, 500-502.

Castells, M. (1996). *The Information Age: Economy, Society and Culture*, Vol. 1, *The Rise of the Network Society*, Malden, MA: Blackwell.

Castells, M. (1998). *The Information Age: Economy, Society and Culture*, Vol. 3, *The End of Millennium*, Malden, MA: Blackwell.

Chin, W. W., Gopal, A., and Salisbury, W. D. (1997). Advancing the theory of adaptive structuration: The development of an instrument to measure faithfulness of appropriation of an electronic meeting system. *Information Systems Research* (8:4), 342-367.

CNN (2002). Experts: Islamic Hackers Ready for Cyber War. http://www.cnn.com/2002/TECH /internet/10/29/tech.islamic.reut/index.html (November 2, 2002).

Cohen, A. (2001). When Terror Hides Online. *Time*, *158*(21), 65.

Deal, T. E., and Kennedy, A. A. (1982). *Corporate Cultures: The Rites and Rituals of Corporate Life.* Reading, MA, Addison Wesley.

de Armond, P. (2001). Netwar in the Emerald City: WTO Protest Strategy and Tactics. In Arquilla, J. and Ronfeldt, D. (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. Santa Monica, CA: Rand, 201-235.

Denning, D. (2001). Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In Arquilla, J. and Ronfeldt, D. (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. Santa Monica, CA: Rand, 239-288.

DeSanctis, G., and Poole, M. S. (1994). Capturing the complexity of advanced technology use: Adaptive structuration theory. *Organization Science*, *5*(2), 121-147.

DeSanctis, G., and Monge, P. (1999). Communication processes for virtual organizations. *Organization Science*, 10(6), 693-703.

Fincham, R. (1992). Perspectives on power: Processual, institutional and 'internal' forms of organizational power. *Journal of Management Studies* 29(6), 741-759.

Garfinkel, H. (1964). Studies of the routine grounds of everyday activities. *Social Problems, 11*(3), 225-250.

Gertz, B. (2002). Terror cells at liberty to strike. *The Washington Times.* http://www.washtimes.com/national/20020918-12894456.htm, (January 21, 2003).

Giddens, A. (1984). *The constitution of society*. Los Angeles: University of California Press.

Goffman, E. (1974). *Frame analysis*. New York: Harper and Row.

Government of Canada (2003). *Canada and Peace Support Operations*. http://www.dfait-maeci.gc.ca/peacekeeping/menu-en.asp, (January 26, 2003).

Granovetter, M. S. (1973). The Strength of Weak Ties. *American Journal of Sociology 78*(6) 1360-1380.

Gulati, R., and Garino, J. (2000). Get the Right Mix of Bricks and Clicks. *Harvard Business Review, 78*(3), 107-115.

Hewlett-Packard Company (2003). *New Wireless Pocket PC Solution Puts Critical Data at the Fingertips of Police.* http://www.hp.com/hpinfo/newsroom/feature_stories/2003/crime03.html (January 21, 2003).

Hansen, M.T., Nohria, N., and Tierney, T. (1999). What's your strategy for managing knowledge? *Harvard Business Review 77*(2), 106-116.

Higgins, A., Leggett, K. and Cullison, A. (2002). How al-Qaeda Put Internet in Service of Global Jihad. *Wall Street Journal*

Hoffman, B. (1993). *"Holy Terror": The Implications of Terrorism Motivated by a Religious Imperative.* RAND Paper P-7834. Santa Monica, CA: RAND.

Houle, S. (2002). Hackers retreat into digital underground. *Computing Canada, 28*(19), http://www.itbusiness.ca/print.asp?sid=50131 (January 19, 2003).

Kaihla, P. (2001). Weapons of the Secret War. *Business 2.0*, November, http://www.business2.com/articles/mag/print/0,1643,17511,00.html (January 21, 2003).

Kaihla, P. (2002). The technology secrets of Cocaine Inc. *Business 2.0*, July, http://www.business2.com/articles/mag/print/0,1643,41206,00.html (January 21, 2003).

Lee, A. S., (1994). Electronic mail as a medium for rich communication: An empirical investigation using hermeneutic interpretation. *Management Information Systems Quarterly, 18*(2), 143-157.

Maitland, I., Bryson, J. and Van de Ven, A. (1986). Sociologists, Economists, and Opportunism. *Academy of Management Review 10*(1), 59-65.

Miller, D.W., Bartkowski, J. P., and Salisbury, W. D. (2000). A Qualitative Analysis of Structural Emergence and Ascendant Leadership in Technological Appropriation. In Ang, S., Krcmar, H., Orlikowski, W., Weill, P. and DeGross, J. I. (Eds.), *Proceedings of the Twenty-First International Conference on Information Systems*, Brisbane, Australia, December 10-13, 588-593.

Moaveni, A. (2002). Bin Laden Hacked! *Time*, http://www.time.com/time/world/printout/0,8816,332914,00.html (January 30, 2002).

Naval Postgraduate School (2002). Terrorist Group Profiles: al-Qaeda. http://library.nps.navy.mil/home/ tgp/qaida.htm, December 13, 2002 (January 22, 2003).

Orlikowski, W. J. (1992). The duality of technology: rethinking the concept of technology in organizations. *Organization Science 3*(3), 398-427.

Orlikowski, W. J. (2002). Knowing in Practice: Enacting a Collective Capability in Distributed Organizing. *Organization Science 13*(3), 249-273.

Ouchi, W. G., (1980). Markets, Bureaucracies, and Clans. *Administrative Science Quarterly*, 129-141.

Polanyi, M. (1967). *The Tacit Dimension*. London: Routledge & Kegan Paul.

Poole, M. S., and DeSanctis, G. (1990). Understanding the use of group decision support systems: The theory of adaptive structuration. In J. Fulk and C. Steinfield (Eds.), *Organizations and communication technology*. Newbury Park, CA: Sage, 173-193.

Rayport, J. F. (2000), Information Resources: Don't Attract, Addict. In D. A. Marchand, T. H. Davenport, and T. Dickson (Eds.), *Mastering Information Management*, London: Prentice-Hall/Financial Times, 42-45.

Reber, A.S. (1993). *Implicit Learning and Tacit Knowledge.* New York: Oxford University Press.

Rouleau, E. (2001). Politics in the Name of the Prophet. *Le Monde Diplomatique*, November, 2001. http://mondediplo.com/2001/11/09prophet?var_s=rouleau (January 21, 2003).

Ronfeldt, D. and Arquilla, J. (2001). What's Next for Networks and Netwars? In Arquilla, J. and Ronfeldt, D. (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. Santa Monica, CA: Rand, 311-361.

Salisbury, W. D., Chin, W. W., Gopal, A. and Newsted, P. R. (2002). Better theory through measurement: Developing a scale to capture consensus on appropriation. *Information Systems Research* 13(1), 91-103.

Sewell, W. H. (1992). A theory of structure: Duality, agency and transformation. *American Journal of Sociology*. 98(1), 1-29.

Standage, T. (1998), *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*, New York: Walker and Company.

Stewart, T. A. (2001a). Six Degrees of Mohamed Atta. *Business 2.0*, December, http://www.business2.com/articles/mag/print/0,1643,35253,00.html (January 21, 2003).

Tenner, E. (1997). *Why Things Bite Back: Technology and the Revenge of Unintended Consequences.* New York: Alfred A. Knopf.

The Economist (2002). Afghan Prisoners: A Transatlantic Rift, January 17, 2002, http://www.economist.com/displayStory.cfm?Story_ID=940904 (January 29, 2003).

Vidal, G. (2002), *Perpetual War for Perpetual Peace: How We Got to Be So Hated*, New York: Thunder's Mouth Press/Nation Book.

Wheeler, B. C. and Valacich, J. S. (1996). Facilitation, GSS, and training as sources of process restrictiveness and guidance for structured group decision making: An empirical assessment. *Information Systems Research*, 7(4), 429-450.

Zack, M. H. (1993). Interactivity and communication mode choice in ongoing management groups. *Information Systems Research*, 4(3), 207-239.

Zanini, M. and Edwards, S. J. A. (2001). The networking of terror in the information age. In Arquilla, J. and Ronfeldt, D. (Eds.). Networks and Netwars: The Future of Terror, Crime and Militancy. Santa Monica, CA: Rand, 29-60.

Postmodern global terrorist groups engage sovereign nations asymmetrically with prolonged, sustained campaigns driven by ideology. Increasingly, transnational criminal organizations operate with sophistication previously only found in multinational corporations. Unfortunately, both of these entities can now effectively hide and morph, keeping law enforcement and intelligence agencies in the dark and on the run. Perhaps more disturbing is the fact that al Qaeda, Hezbollah, FARC, drug cartels, and increasingly violent gangs--as well as domestic groups such as the Sovereign Citizens--are now join Main Character Index > Villainous Organizations > Criminals & Terrorists â€¦Â International and Transnational Organizations. Batroc's Brigade. Georges Batroc.Â An anti-alien and anti-government hate group that has came into formation months after Terrigen went widespread with plans to eliminate Inhumans and their supporters. Equal-Opportunity Evil: They seem to recruit anyone who has anti-Inhuman agendas, regardless if they're Caucasian, Asians or Africans. Expy: This interpretation of the Watchdogs is essentially the MCU equivalent of the Friends of Humanity and other similar groups, albeit focused on Inhumans rather than Mutants. Faceless Mooks: They cover their faces in masked helmets that resemble a mixture of a skull and an attack dog. As terrorist groups are usually engaged in a long war of attrition, terrorist orga- nizations need ongoing support and funds to ensure they can maintain their activi- ties. In fact, one of the main sources of funding for many terrorist organizations is criminal activity: smuggling, counterfeiting, extortion, and narcotics. At the begin- ning of the twenty-first century, the threat of international terrorism grew with the spread of Global Jihad terrorism. Made up of complex networks of hierarchal terrorist organizations, proxy and affiliate organizations, local and