The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

THEME ARTICLE

On the imbalance of the security problem space and its expected consequences

Konstantin Beznosov
Department of Electrical & Computer Engineering, University of British Columbia, Vancouver, Canada, and
Olga Beznosova
Department of Political Science, University of British Columbia, Vancouver, Canada

Abstract

Purpose – This paper aims to report on the results of an analysis of the computer security problem space, to suggest the areas with highest potential for making progress in the attacker-defender game, and to propose questions for future research.

Design/methodology/approach – The decomposition of the attacker-defender game into technological, human, and social factors enables one to analyze the concentration of public research efforts by defenders. First, representative activities are selected, then each activity is mapped into the technological, human and social (THS) basis. Afterwards, citation databases are used to estimate the relative volume of publications on each selected activity in the science and engineering communities. Finally, drawing on a number of relevant theories in organizational theory, sociology, and political science, avenues for exploring the social dimension by the defenders are discussed.

Findings – The analysis suggests that over 94 percent of the public research in computer security has been concentrated on technological advances. Yet attackers seem to employ more and more human and social factors in their attacks. The social organization of the attackers allows them to achieve the results not possible otherwise, shifting the balance in their favour. It is suggested that the scope of research should be broadened, to involve organizational behavior and structure as well as social capital aspects that are currently not high on computer security research agenda.

Research limitations/implications – The queries limit the search to public content written in the English language only. Since the authors are concerned with the relative (rather than absolute) volume of each activity, it is an open question whether this limitation biases the results.

Practical implications – As the arms race in computer security progresses, social factors may become or already are increasingly important. The side that capitalizes on them sooner may gain the competitive advantage.

Originality/value – A simple method for gauging the focus of research efforts in the computer security community and for considering computer security problem space through the lens of social sciences is developed.

Keywords Computer applications, Data security, Human failure

Paper type Viewpoint

Information Management & Computer Security
Vol. 15 No. 5, 2007
pp. 420-431

0968-5227
DOI 10.1108/09685220710831152

The authors would like to thank anonymous reviewers for their constructive and helpful comments, Lee Iverson for feedback on an earlier version of this paper, and Craig Wilson for improving the readability of this paper. The first author has been in part supported by the Canadian NSERC Strategic Partnership Program, grant STPGP 322192-05.

1. Introduction

Computer security is a complex subject whose interdisciplinary nature is clearly delineated by Anderson (2001). To generalize the famous quote by Needham and Lampson about cryptography, we believe that "people who think their security problem can be solved with only technology do not understand the problem and do not understand the technology". But how much attention is paid by both attackers and defenders to aspects of computer security that are not technological? If these other aspects are not being explored, what are the implications?

This paper reports on the results of our analysis of the computer security problem space and suggests the areas with highest potential for making progress in the attacker-defender game. To analyze the problem space, we qualitatively decomposed the major activities in computer security on the basis of technological, human, and social (THS) factors, then estimated the proportions of these activities in research on science and engineering world-wide as well as the attention to them paid by the press.

We use the term "activity" instead of "area" or "functionality" (or similar terms) to highlight our focus on offensive (e.g. social engineering, phishing) and defensive (e.g. cryptography, intrusion detection, information assurance, access control) practices, as well as those aspects of computer security that can be employed by either side (e.g. economics and politics of security).

Our simple, but hopefully symptomatic, estimation of world-wide research activities related to several major areas of computer security indicates that over 94 percent of these activities have so far concentrated on the technological dimension (e.g. cryptography, access control, intrusion detection, malware). Activities focused on the human and social aspects of the security problem account for less than 6 percent in total. Although the way we estimated the volumes is unlikely to sustain any criticism from statisticians, we do believe the results are representative.

These results, for one, underscore the popular notion that in the last 40 years, progress in computer security has been mostly due to technological advances. The results of our queries on Google News Archives – which indicate that "public" opinion rates social and human dimensions of security significantly higher than the share of the corresponding public research – point at least to the mismatch between the public concerns and the focus of the researchers. Drawing on recent results from other disciplines, we believe that as the computer security arms race progresses, social factors may become increasingly important. In fact, the next big spiral in this arms race may very well be due to advances in the social dimension. Arguably, potential advantages of the social dimension have already been exploited by attackers, as demonstrated by numerous cases of social engineering (Mitnick *et al.*, 2002; Gordon, 1995). It is not clear who, attackers or defenders, will take the lead. The other side will have to catch up.

The rest of the paper is organized as follows. Section 2 describes our analysis of the computer security problem space and discusses the expected consequences of the identified imbalance. Section 3 discusses social dimensions of computer security and considers the application of some methods and results from social sciences to it. Section 4 discusses avenues for future research. Section 5 concludes the paper.

2. The imbalance of the security problem space

While the dominant role of the technology in the research on computer security can be easily established by, for example, browsing through the proceedings of major professional and research conferences devoted to security, we wanted to validate popular beliefs about the bias towards technology, using a more systematic approach. This section describes a simple study we performed, the results collected, and our interpretation of the results.

2.1 Methods

To gain an understanding of which aspects (THS) of the computer security have been the focus of the research community, we first selected representative activities of the attacker-defender game. We then mapped each activity into THS basis. Owing to the space limitation of this paper, we do not discuss the method and results of our mapping in detail. Finally, we used Web of Science[1] and Engineering Village's Compendex[2], and Inspec[3] citation databases to estimate the relative volume of publications on each selected activity in the science and engineering communities. The rest of this section describes the activity selection and steps of our analysis.

The set of selected computer security activities is listed in the left-most column of Table I. This list is not intended to be comprehensive, and some of the selected activities do overlap. For instance, cryptography is directly employed in some access control solutions, and information assurance does rely on access control and cryptography. However, since the purpose of this analysis was to uncover global trends, signs of which have accumulated in the scientific and engineering publications, we believe that the selected activities are representative of the major focus areas. After selecting the activities, we performed the mapping.

Our premise in mapping was that most computer security activities – performed by either attackers or defenders of computer systems – can be viewed as consisting of components related to either THS aspects, and therefore can be broken down on the THS basis[4]. By technological we refer to all aspects of computer security that involve purely technological solutions. We use the term human aspects to refer to such factors as human psychology, physiology, and cognition at the individual level. By social aspects we refer to those factors that are due to interactions among more than one person in social or formal organizations and within wider social context. Using our judgment, we mapped the selected activities on the THS basis. Figure 1 graphically shows the results of our mapping.

In order to estimate the relative weight of each activity in the public research community, we determined the percentage of indexed publications related to each activity, according to the number of entries returned by the search engines of Web of Science (2007) and Engineering Village (2007) in response to our queries. As the query syntax for all three data sources was similar, the second column of Table I lists only Engineering Village version of the search queries for each activity. To be safe, we aimed to construct queries that were liberal (i.e. returned more rather than fewer results) for activities with significant social and human aspects, and conservative for technology-centric activities, according to the mapping described in the next section.

To avoid double-counting of those publications that were returned for more than one query in the same THS group, we also obtained statistics on each of these three groups by making a single query that comprised all queries in the group. We were

Activity	Engineering village search query[a]	Relative weight (percent)[b] Google news archives	Web of science	Engineering village
Technology-centric cumulative		*58.3*	*94.2*	*95.6*
Cryptography	Cryptography or cryptographic or encryption or decryption	30.5	90.2	79.1
Malware	Malware or "computer worm" or "computer virus"	14.4	1.6	1.9
Information assurance	Computer and ("security assurance" or "information assurance") not financial not social	0.7	0.2	1.2
Intrusion detection	Intrusion and detection and computer and security	3.9	1.5	5.5
Access control	("Access control" or authorization) and computer and security	8.7	1.0	8.0
Human-centric cumulative		*30.4*	*2.3*	*2.3*
Usable security	security and (usability or usable or HCI)	17.6	1.9	1.8
Phishing	Phishing	12.6	0.3	0.4
Shoulder surfing	"Shoulder surfing"	0.2	0.04	0.03
Social-centric cumulative		*11.4*	*3.2*	*2.1*
Social engineering	"Social engineering"	5.3	2.3	0.2
Politics and security	(Politics or bill or legislation or regulation) and ("information security" or "computer security")	4.3	0.2	1.0
Economics of security	(Economics and ("information security" or "computer security")) or "security economics"	0.5	0.1	0.2
Organizational and social	(Security and "human factor") or "security awareness" or "security training" or "security culture" and (computer or information)	1.2	0.6	0.7
Total for individual types of activities		100	100	100

Notes: [a]Description of the queriy format can be found at Engineering Village (2007); [b]as of April 8, 2007

Table I.
Search queries and the results for representative keywords

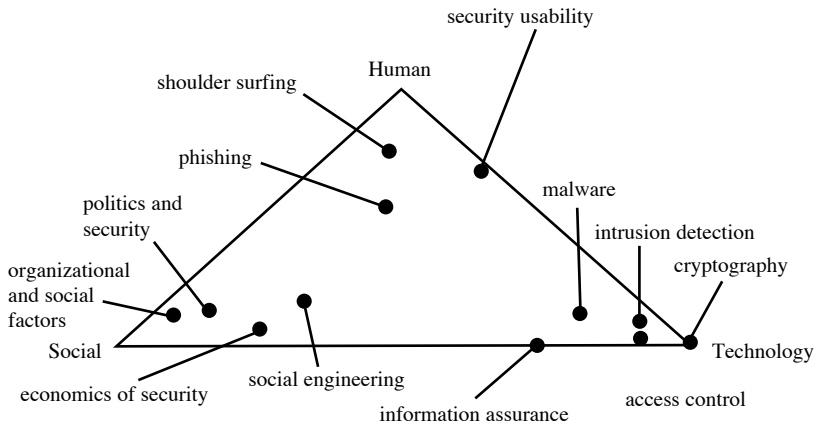

Figure 1.
Activities mapped on the THS basis

unable to do so for Google News Archives due to the limitations on the search string length. The queries limited our search to public content written in the English language only. Since, we were concerned with the relative (rather than absolute) volume of each activity, it is an open question whether this limitation biased the results.

2.2 Results

The percentage of scientific or engineering publications related to each type of activity found through Web of Science and Engineering Village (rounded to tenths of percentile) are listed in the two right-most columns of Table I. Figure 1 shows each activity mapped on the THS basis.

When we grouped activities into technology-centric (cryptography, access control, intrusion detection, information assurance, and malware), human-centric (security usability, phishing, and shoulder surfing), and social-centric (economics of security, social engineering, politics of security, as well as organizational and social factors), the first group consistently accounted for over 94 percent of indexed publications in scientific and engineering outlets, the human-centric and the social-centric groups enjoyed no more than 2-3 percent each.

For comparison, the table also shows statistics of these categories' popularity in the Google News Archives search engine, which likely correlates with the degree of recent press coverage. Table I reveals the divergence between the results of the queries from "popular" discussions on Google News Archives and those in the research community. While in the latter, human and social-centric cumulative scores were just 2-3 percent each, in the former it was significantly higher – 11 and 30 percent of queries returned references to the social and human dimension of security, respectively.

2.3 Discussion

The results of our analysis indicate that the focus of public research related to computer security has been overwhelmingly focused on technological aspects, leaving human and social dimensions mostly uncharted. This imbalance between technology-centric and human/social centric activities can be interpreted in a number of ways. Computer security (including information security) has from its

beginnings been a technology-focused game played by attacker(s) against defenders(s). One can argue, therefore, that the current focus on technology is normal and will continue on both sides in the foreseeable future. Our view is different.

We believe that the attackers have become increasingly aware of the importance of human and social aspects in the attacker-defender game. It is indirectly confirmed by Fathi, Microsoft's Vice President for the Windows core operating system, who stated that "most users encounter PC security issues because they fall for social engineering tactics ..." (Hines, 2007). The testimony before the US Congress by arguably "the world's most famous hacker" Kevin Mitnick – who then said "I was so successful in that [social engineering] line of attack that I rarely had to resort to a technical attack" (The Associated Press, 2000) – confirms that it is often easier for the attackers to exploit human and social weaknesses of the defenses than to defeat the technological countermeasures. For research in computer security to sustain the arms race, it ought to explore the social dimension of the problem space.

3. Social dimension

We define social aspects of security as those that are exclusively due to interactions among more than one human actor on either side of the attacker-defender game. Of course, the boundaries of such categories can sometimes be fuzzy. Some may be relatively easy to classify, e.g. economics of security qualify as social dimension and usability of security controls as human aspect of the problem space. Other phenomena, for example social engineering, may be more difficult to label. While the success or failure of a particular social engineering attack depends on actions of a particular human being, these actions are determined by a larger context of habitual and widely accepted organizational practices and societal norms, which emerged together with the development of interfaces and software. Therefore, to disarm a social engineering attacker this context could be altered through training or awareness campaigns. Hence, the solution might have been located on the social plane of the problem space.

We suggest that taking into account social and organizational matters may be important for computer security research in order to advance in the attacker-defender game. The examples below illustrate that when attacks take social factors into account, the magnitude and scale of their impact may be increased manifold, leaving the other side to cope with it. Consequently, when organizational and social factors are left unattended in certain situations, the outcomes may be quite disastrous.

Intuitively, it seems that in the attacker-defender game, social factors may bring competitive advantage to the side that employs them first. The following examples cited by Denning (2001, p. 257) provide a number of illustrations of how exactly social factors may bring to the table what was not predicted and planned for by the defenders.

In 1999 protests were set up to coincide with a meeting of the G8 in Cologne, Germany. A group called J18 coordinated the protests through a web site inviting people to plan individual actions focusing on disrupting "financial centres, banking districts, and multinational corporate power bases." Hackers from Indonesia, Israel, Germany, and Canada simultaneously attacked the computers of at least 20 companies, including the Stock Exchange and Barclays. More than 10,000 attacks were launched over a five-hour period (Ungoed-Thomas and Sheehan, 1999).

On June 15, 1999, the Electronic Disturbance Theater organized an act of Electronic Civil Disobedience to stop the war in Mexico. The suggested action was for people

using computers to simply point their web browsers to a specific URL at a particular time. By directing web browsers toward the Zapatista FloodNet URL during this time period, people joined a virtual sit-in. Their individual computers began sending re-load commands over and over again for the duration of the time they were connected to FloodNet. The results of the June 18 Electronic Disturbance Theater virtual sit-in were that the Zapatista FloodNet URL received a total of 18,615 unique requests from people's computers in 46 different countries. The repeated re-load command of the individual user – multiplied by the thousand engaged – clogged the internet pathways leading to the targeted web site. In this case on June 18, FloodNet was directing these multiple re-load browser commands to the Mexican Embassy in the UK. The global Zapatista FloodNet action was the first that the Electronic Disturbance Theater called for in 1999. The group began in the spring of 1998 and launched a series of FloodNet actions directed primarily against web sites of the Mexican Government, but action targets also included the White House, the Frankfurt Stock Exchange, the Pentagon (Wray, 1999).

Individuals acting alone or in small groups have used network flooding tools to disable internet servers. During the Kosovo conflict, Belgrade Hackers conducted such attacks against NATO servers. Bombarding NATO's web server with "ping" commands, they caused line saturation of the targeted servers (Allison, 1999).

To be sure, attackers can exploit social aspects of security without human buy-in and active participation. The best examples are flooding and spamming attacks that use botnets – collections of compromised end-user PCs remotely controlled by attackers. However, we argue that the social dimension is crucial even in botnets. The recent trend among attackers is to create botnets by implanting malware on victim's computers using "drive-by download" attacks – which rely on the combination of vulnerabilities in web browsers and social engineering tricks, according to Viega (2007) the Chief Security Architect of a major antivirus and computer security company McAfee. He predicts these attacks to become more and more cost effective, as the average level of user security knowledge declines due to the growth of the broadband internet penetration, which is expected to exceed 50 percent among US households in 2007 (Parks Associates, 2007).

As the above discussion suggests, social organization of the attackers allowed them to achieve the results not possible otherwise, shifting the balance in favor of the protesters and away from the defenders of the computer systems. A number of social science disciplines, including organizational theory, sociology, and political science, developed theories that enhance our understanding and management of social aspects of conflictual and competitive situations. In the remaining part of the section, we suggest to broaden the scope of research to involve organizational behavior and structure as well as social capital aspects that are currently not high on computer security research agenda.

3.1 Organizational processes and behavior

Probably one of the most influential schools of organizational thought, referred to as the decision-making or behavioral school, was developed by Simon and March in 1950s. The school focuses on the connection between bounded rationality and behavioral structure, demonstrating that because individuals and organizations are limited in knowledge and computational abilities, they have to rely upon habits,

routines, and other forms of programmed behavior in making decisions. The critical point to understand about organizations is that structure arises out of cognitive limitations. Allison's (1971) one of the most influential books in modern politics, analyses the Cuban missile crisis to demonstrate how certain international security events can be understood differently based on the model employed. One of Allison's models, the organizational process model, is built around Simon-March tradition, which emphasizes bounded rationality and routine behavior of the major organizations involved in the crisis: the state department, the Soviets, the military, etc. (Moe, 1991).

3.2 Organizational structure

Another area of research concerns structural characteristics of organizations and is quite often employed in the study of terrorism and organized crime. For example, Arquilla *et al.* (1999) conducted a study of the impact of ongoing information revolution and networks on terrorist capabilities, and how this development may be associated with a move away from emphasis on traditional, episodic efforts at coercion to a new view of terror as a form of protracted warfare. They suggest the term netwar to refer to:

> . . . an emerging mode of conflict and crime at societal levels, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command. Thus, information-age netwar differs from modes of conflict and crime in which the protagonists prefer formal, standalone, hierarchical organizations, doctrines, and strategies, as in past efforts (Arquilla *et al.*, 1999, p. 47).

Critical here is the attention to a change in organizational forms along with strategies and tactics that terrorists (or other attackers for that matter) use, and the implications this change has for those who design protection measures. According to Arquilla and Ronfeldt (2001), organizational purposes affect the suitability and effectiveness of various types of social structures. For example, Arquilla and Ronfeldt illustrate how different organizational structures – a chain network, a "star" or hub network, and an all-connected network – can aid organizations in achieving certain objectives, such as information sharing, communications, cooperation, as well as their defensive and offensive potential. In a computer security attacker-defender game, security administrators may find themselves in a disadvantaged position if they are not prepared to deal with changing organizational forms and tactics of the attackers' teams.

Considering the context and environment in which the game takes place is imperative for determining the actors' chances of success. For example, research on business organizations (Saetre, 1996; Boudreau, 1998) and criminal networks (Williams, 2001) demonstrates that in the globalizing world, the constraints, rigidities, and inefficiencies of hierarchical organizational structures rendered them inadequate and forced the competing organizations to restructure. It was shown that actors could gain competitive advantages in this changing environment through what was sometimes called "agile networks" (Saetre, 1996) or "virtual organizations" (Boudreau, 1998). To accommodate environmental constraints and take advantage of opportunities, considerable emphasis in these organizations is placed on flexible internal communication networks, strategic connections, the ability to respond rapidly to external opportunities and challenges, rapid information processing, and quick decision making (Lewin and Stephens, 1993; Saetre, 1996).

3.3 Culture, norms, social capital

While the right organizational routines and structure may be necessary for gaining competitive advantage, they may not be sufficient. Researchers and practitioners alike increasingly recognize that social capital, which includes both structural and attitudinal components of social organization, is critical for effective functioning of organizations and for gaining competitive advantage. It has been demonstrated by research in sociology (Coleman, 1990), conflict studies (Colletta and Cullen, 2000) and business (Saetre, 1996; Handy, 1995) that organizations with higher levels of trust, horizontal cooperation, and loyalty show better performance and efficiency than those that are deficient in these factors.

As this brief overview of the literature suggests, under the conditions of conflict and competition, achievements in the technological dimension of the THS basis only may not necessarily give attackers or defenders sufficient advantage to stay on top of the game. The intervening factor may well be the interaction between the social and organizational structures of the actors, the actors' goals, and the broader environmental context, which could be responsible for the success or failure of actors' strategies. What this discussion suggests for computer security research, is that studying social dimensions of information security problem space will allow the computer security community to better understand existing problems and design more effective solutions for some of them.

4. Suggestions for further research

Drawing on the discussion in the previous sections, we suggest a number of areas for further research: organizational processes, behaviors, and structures, as well as organizational culture, and societal norms.

One potentially fruitful research agenda concerns the relationship between organizational processes and behavior and the effectiveness of security defenses. For example, one could study decision-making processes and operational routines within organizations to better understand how they influence security posture of the organizations. In particular, taking into account business goals of the defenders, the ways in which security-related decisions are made and carried out, and the structure of formal and informal cooperative relationships within defender's organization, what kinds of processes meet defender's objectives best?

Another interesting direction is the exploration of the relationship between organizational structures and security. As mentioned above, there is a wide variety of organizational structures, from hierarchies to flexible task-specific networks. For example, Botta *et al.* (2007) find that the IT security job is distributed across multiple employees, often affiliated with different organizational units or groups within a unit and responsible for different aspects of security, typically with single coordinator, who is not necessarily higher on the organization ladder than the other group members. Comparing security postures and effectiveness of security programs within organizations, one could determine what kinds of organizational structures are more effective for defending against which security threats.

If to further this direction, the relationship and interaction between attackers' and defenders' organizational structures could be investigated. Is it possible to study models of attackers' organizations, and determine the relationship between attacker's organizational structure and the effectiveness of their attacks? What kinds of countermeasures can be employed by defenders to effectively oppose the attackers, given the organizational structure of the two?

As discussed in the previous section, organizational culture, norms, and social capital might play an important role in the effectiveness of security measures. While Knapp *et al.* (2006) find positive correlation between top management support and security culture as well as security policy enforcement, further investigation is needed to establish the causal relationship between organizational cultures, norms, and social capital and the effectiveness of organizational security strategies and programs.

Social aspects of security do not stop at the doorstep of specific organizations. End-user behaviors intertwine inextricably with the overall level of individual security. However, as more and more users connect to internet through high-speed channels, the network effect results in the exponentially increasing impact of personal security behavior of individual users on others. Even worse, the higher penetration of broadband internet connections in the households of modern societies also results in the lowering average level of personal security "hygiene". It is thus useful to look at wider societal aspects of security promotion mechanisms, such as education, awareness building, and policy. For example, what kind of mechanisms would be effective to increase awareness about security risks, and personal security hygiene? Such a study can benefit greatly by borrowing from other disciplines. Some of the examples could be the development of societal norms and policies pertaining to recycling, seat belt use, as well as drinking and smoking.

5. Conclusion

The bulk of the published research in the computer security has so far been in the technological dimension. The human and social aspects are currently largely neglected in computer security research. As the arms race in computer security progresses, social factors may become or already are increasingly important. The side that exploits these factors sooner may gain competitive advantage, since by employing different organizational structures and processes and adapting better to the wider social context, either side can gain sufficient advantages even when lacking in technological capabilities.

The next big spiral in the computer security arms race may very well be due to advances in the social dimension. It is not clear who, attackers or defenders, will be first to fully exploit this area. The other side might end up in catch-up mode, as the modern history of social engineering, phishing, and terrorism illustrates.

Notes

1. Web of Science (2007) is a citation database of approximately 8,700 research journals.
2. Compendex is a bibliographic database of engineering research that contains over nine million references and abstracts from 1969 to present taken from over 5,000 engineering journals, conferences and technical reports.
3. Inspec is a bibliographic database that contains over eight million bibliographic records taken from 3,500 scientific and technical journals and 1,500 conference proceedings. Approximately 330,000 new records are added to the database annually.
4. We use the term basis in this paper by analogy with the vector space basis, which is a list of vectors $(\mathbf{v}_1,\mathbf{v}_2, \equiv ,\mathbf{v}_n)$ in vector space $\mathbf{V}$ such that for any $\mathbf{v} \in \mathbf{V}$ it can be represented as a composition of the vector space basis: $\mathbf{v} = \alpha_1 v_1 + \alpha_2 v_2 + \ \equiv \ + \alpha_n v_n$. The dimension of $\mathbf{v}$ is n.

References

Allison, G.T. (1971), *The Essence of Decision: Explaining the Cuban Missile Crisis*, Little Brown, Boston, MA.

Allison, R. (1999), "Belgrade Hackers Bombard MoD website in 'first' internet war", *PA News*, March 31.

Anderson, R.J. (2001), *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, New York, NY.

Arquilla, J. and Ronfeldt, D. (2001), "The advent of netwar (revisited)", in Arquilla, J. and Ronfeldt, D. (Eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Rand Corporation, Santa Monica, CA, pp. 61-97.

Arquilla, J., Ronfeldt, D. and Zanini, M. (1999), "Networks, netwar, and information-age terrorism", in Lesser, I.O., Hoffman, B., Arquilla, J., Ronfeldt, D., Zanini, M. and Jenkins, B.M. (Eds), *Countering the New Terrorism*, Rand Corporation, Santa Monica, CA.

(The) Associated Press (2000), "Noted Hacker speaks before senate panel", available at: http://partners.nytimes.com/library/tech/00/03/biztech/articles/02hack.html

Botta, D., Beznosov, K., Iverson, I., Fisher, B., Fels, S. and Werlinger, R. (2007), "Studying IT security professionals: research design and lessons learned", position paper for the CHI Workshop on Security User Studies: Methodologies and Best Practices.

Boudreau, M-C. (1998), "Going global: using information technology to advance the competitiveness of the virtual transnational organization", *Academy of Management Executive*, Vol. 12 No. 4, pp. 120-8.

Coleman, J. (1990), *Foundations of Social Theory*, Harvard University Press, Cambridge, MA.

Colletta, N.J. and Cullen, M.L. (2000), *Violent Conflict and Transformation of Social Capital: Lessons from Cambodia, Rwnada, Guatemala and Somalia*, World Bank, Washington, DC.

Denning, D. (2001), "Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy", *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Rand Corporation, Santa Monica, CA, pp. 239-88.

Engineering Village (2007), "Engineering village", available at: www.engineeringvillage2.org/

Gordon, S. (1995), "Social engineering: techniques and prevention", *Proceedings of the 12 World Conference on Computer Security, Audit and Control*, Elsevier, London, pp. 445-51.

Handy, C. (1995), "Trust and the virtual organization", *Harvard Business Review*, Vol. 73 No. 3, pp. 40-50.

Hines, M. (2007), "Vista aims to stop Hackers' social engineering ploys", available at: www.eweek.com/article2/0,1895,2084631,00.asp

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Nelson Ford, F. (2006), "Information security: management's effect on culture and policy", *Information Management & Computer Security*, Vol. 14 No. 1, pp. 24-36.

Lewin, Y. and Stephens, C.U. (1993), "Epilogue: designing postindustrial organizations: combining theory and practice", in Huber, G.P. and Glicks, W.H. (Eds), *Organizational Change and Redesign*, Oxford University Press, New York, NY, pp. 393-410.

Mitnick, K.D., Simon, W.L. and Wozniak, S. (2002), *The Art of Deception: Controlling the Human Element of Security*, Wiley, New York, NY.

Moe, T. (1991), "Politics and the theory of organization", *Journal of Law, Economics, and Organization*, Vol. 7, pp. 106-29.

Parks Associates (2007), "US residential broadband penetration to exceed 50% in 2007", available at: www.parksassociates.com/press/press_releases/2007/dig_lifestyles1.html

Saetre, S. (1996), "The agile network: a model of organizing for optimal responsiveness and efficiency", paper presented at The Fifth National Agility Conference.

Ungoed-Thomas, J. and Sheehan, M. (1999), "Riot organisers prepare to launch cyber war on city", *Sunday Times*, August 15.

Viega, J. (2007), "Malware in the real world", paper presented at The 14th Annual Network & Distributed System Security Symposium, Invited Talk, Internet Society, San Diego, CA.

Web of Science (2007), "Web of science web site", available at: www.isiknowledge.com

Williams, P. (2001), "Transnational criminal networks", in Arquilla, J. and Ronfeldt, D. (Eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Rand Corporation, Santa Monica, CA, pp. 61-97.

Wray, S. (1999), "June 18: the virtual and the real action on the internet and in Austin, Texas/Zapatista Floodnet and Reclaim the streets".

Corresponding author
Konstantin Beznosov can be contacted at: beznosov@ece.ubc.ca