CYBERPSYCHOLOGY & BEHAVIOR
Volume 6, Number 2, 2003

Flow-Based Model of Computer Hackers' Motivation

ALEXANDER E. VOISKOUNSKY, Ph.D., and OLGA V. SMYSLOVA, Ph.D.

ABSTRACT

Hackers' psychology, widely discussed in the media, is almost entirely unexplored by psychologists. In this study, hackers' motivation is investigated, using the flow paradigm. Flow is likely to motivate hackers, according to views expressed by researchers and by hackers themselves. Taken as granted that hackers experience flow, it was hypothesized that flow increases with the increase of hackers' competence in IT use. Self-selected subjects were recruited on specialized web sources; 457 hackers filled out a web questionnaire. Competence in IT use, specific flow experience, and demographic data were questioned. An on-line research was administered within the Russian-speaking community (though one third of Ss are non-residents of Russian Federation); since hacking seems to be international, the belief is expressed that the results are universal. The hypothesis is not confirmed: flow motivation characterizes the least and the most competent hackers, and the members of an intermediate group, that is, averagely competent Ss report the "flow crisis"—no (or less) flow experience. Two differing strategies of task choice were self-reported by Ss: a step-by-step increase of the difficulty of choices leads to a match of challenges and skills (and to preserving the flow experience); putting choices irrespective of the likelihood of solution leads to a "flow crisis." The findings give productive hints on processes of hackers' motivational development. The flow-based model of computer hackers' motivation was developed. It combines both empirically confirmed and theoretically possible ways of hackers' "professional" growth.

INTRODUCTION

COMPUTER HACKERS, taken as a target group seem problematic to be investigated, mainly due to organizational and procedural difficulties. Hackers tend to stay anonymous; even when pooled in teams they would not let others enter into their underground communities. Hackers' behavioral patterns as presented and discussed in the media are supposedly far from the real ones.

Professionals most sensitive to computer hackers' behaviors are their counter-partners—computer security experts. Not that they need to know a hacker as a psychological type, although some security experts are known to be former hackers. Sociologists and anthropologists provide an expanding source of knowledge about specific hackers' communities. Social researchers express professional interest in group norms, patterns of verbal exchanges and distant forms of hackers' social life, but of course not in psychology of hacking.

The focus on the human side of hacking might be viewed quite rarely—when a hacker is taken to court. Thus, up to now solely servants of Law—judges, criminologists, lawyers, police officers—dealt with hackers as persons. Their professional standpoint is specific, and restricted to a sample of hackers who were unable to escape being caught.

No doubt, psychologists might present a realistic view of computer hackers' personalities. To the best of the authors' knowledge hackers have not been thoroughly investigated by psychologists, but

Psychology Department, Moscow State University, Moscow, Russia.

for Turkle's study made two decades ago.[1] The majority of hackers grew up, or were born since that time. In this sense, the modern generation of hackers is really anonymous.

Technical and juridical means are universally accepted to resist hackers' attacks. To our view, alternative ways might be promising and are worth trying. For example, adequate educational programs might work quite well to reduce recruitment of new hackers, if not diminish their most destructive takedowns. Education needs to be based on psychological data; police actions and firewalls should not substitute psychological research.

Researchers have only vague ideas: what really pushes hackers to hack, i.e. what is their motivation. Although this is the key issue, too little efforts have been made to understand motivation of the modern generation of hackers. Some self-reported motives of hacking are presented by Taylor,[2] of illegal use of computers and the Internet—by McGuire and colleagues.[3] Since only anecdotal and self-reported evidences are available, we might conclude that research in this problem area is not advanced enough. This paper presents an empirical research of the hackers' motivation.

Hackers and motivation

Hackers were presented in 1960s as smart and competent enthusiasts, interested exclusively in computers and software.[4] Their dominant motivation was reportedly cognition, they were fully engaged both in productive and non-productive projects. The latter include for example some ambitious Artificial Intelligence projects.[4] Many people believe that the best software products ever created were composed by hackers.[5,6] For hackers, the use of computers often replaced universal qualities of life. As Sterling[6] wrote, "hacking could involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit". At early stages of computerization, many competent programmers outside the hackers' community shared these views.[7] Knuth[8] expressed the idea that "it is possible to write grand programs, noble programs, truly magnificent ones!"

Since that time, hackers evolved in many ways. Usually, the following generations are distinguished: the first generation of pioneers who were involved in the development of the earliest software products and techniques of programming, the second generation of those who developed first PCs and brought computers to masses, and the third generation who invented computer games and made them available to public.[5] Taylor[2] added the fourth generation of hackers "who illicitly access other people's computers." Beginning with the earliest publications,[1,4] it was often stressed that hackers find their activity valuable.

Needless to mention, the changes from computer pioneers to computer burglars were not spontaneous. Influential cultural innovations were first introduced by phone phreaks, then were caused by gradual spreading of PCs and later of the Internet, and finally by media reports about hackers' evil performance—all this too often led to transformations of sophisticated computer specialists into computer pirates. These pirates are usually called hackers—the newest generation of them.

Media portrays modern hackers as pirates, money and documentation stealers, and creators of computer viruses; this view is partly shared by analysts.[2,6] In the sources compiled and updated by hackers themselves[9] illegal intentions and actions are attributed to crackers—"bad guys" who stay outside (though most people believe within) the hackers' community.

Hackers' community is not uniform indeed: there are various sub-groups under the hacker umbrella. Since hackers obviously differ, a number of classifications were suggested.[6,10,11] The subgroups are classified dependent on their expertise, areas of interests (e.g., software, hardware, cell phones, the Internet) and behavior patterns. Subgroups vary from novices to professionals. For instance, Rodgers[12] distinguishes seven groups of hackers: tool kit/newbies, cyber-punks, internals, coders, old guard hackers, professional criminals, and cyber-terrorists. Tool kit/newbies are newcomers to hacking who rely on previously prepared ready-to-use pieces of software (tool kits), and on web instructions "how-to." Cyber-punks are capable of writing their own pieces of software, but their knowledge is rather limited; they also engage in malicious acts, such as defacing web pages, sending junk mail, stealing credit card numbers. Internals are ex-employees whose attacks are based on precise competence in principles of computer security practiced at their former organizations. Coders are highly skilled; they write new programs so that all the others might use them for hacking. The old guard hackers are those who are most qualified and try to follow the ideology of the first-generation-hackers and are interested in the intellectual/cognitive side of hacking.[12] The other two groups of hackers fully correspond to their indications.

Motivation is among the most important characteristics of human behavior. Too little is known about the hackers' motivation. When interviewed,

hackers often report that while hacking they experience full involvement in the task and think of no rewards.[2,11] This is an important hint of the hackers' supposed motivation. Based on hackers' self-reports, we assume that a sort of intrinsic motivation is characteristic for hackers—at least for many of them (probably not for internals). Intrinsic motivation is the tendency to engage tasks for their own sake; one finds these tasks interesting or challenging. On the contrary, extrinsic motives, such as rewards are task-unrelated.[13]

Intrinsic motivation has long been underestimated by psychologists. Only recently, it was realized that extrinsic stimuli and rewards are not the only motives that direct human behavior effectively. As Csikszentmihalyi[14] formulates it, even "antropological evidence shows that there are cultures in which material goals do not have importance we attribute to them."

The most elaborated actual concept of intrinsic motivation is the flow theory/paradigm originated by Csikszentmihalyi.[15] Flow means that an action freely follows the previous action, and the process is in a way unconscious; flow is accompanied by positive emotions and is self-rewarding. A person "experiences it as a unified flowing from one moment to the next, in which he is in control of his actions, and in which there is a little distinction between self and environment, between stimulus and response, between past, present, and future."[14] Of crucial importance is M.Csikszentmihalyi's[14] statement that the main antecedent of flow is precise matching of someone's skills and task challenges. Moreover, both skills and challenges should not be too low, otherwise this way of matching leads to apathy: chewing bubble gum is "an extreme example."[16] Flow is placed at the cutting edge of a person's skills, and it is a moving target: increasing skills need an increase of challenges to save the precise matching, and a choice of high challenges leads to an update of skills; after a period of learning the precise matching happens anew.

The concept of flow, and of optimal experience[17] derived from it proved to be useful to interpret motivations of teachers and students, of people engaged in sports and of artists, of IT professionals, and e-shoppers.[14,18–24] Flow might accompany almost every sort of behavior, and some activities specially facilitate flow: these are games, sports, and what is called "creativity in general."[14] Since we suppose that hackers are intrinsically motivated, it looks likely that they experience flow.

Investigation of flow in activities associated with computer use and specifically with the Internet use started in 1990s.[16] Internet users are known to experience flow,[16,20] as well as MUD players,[19] computer-mediated communicators[22] and e-shoppers.[24] Since hackers are known to be heavily using computers and the Internet, Beveren hypothetically supposed that hackers might experience flow.[20] He introduced a model of hacker's development, based on Rodger's taxonomy of hackers. This model has not been proved empirically.

Hoffman and Novak[16] found that the more experienced users report to have higher level of flow, compared to inexperienced ones. This result seems to be valuable. Since flow is believed to be important for hackers and to motivate them, we hypothesize that the more qualified and competent hackers experience flow more often than less qualified hackers.

Russian hackers are often believed to be creative and competent. Several of them were arrested in the USA (Vladimir Levin, Dmitri Sklyarov, Alexey Ivanov, Vasiliy Gorshkov). Within Russia, on the contrary, they enjoy the advantages of being informally accepted as heroes, not criminals.[21] We take as granted that hacking is a universal activity with few (if any) ethnic/geopolitical differences. Thus, research on hackers' motivation was planned and administered within the Russian-speaking community of hackers; we believe this does not diminish the universality of the results.

MATERIALS AND METHODS

Since hackers tend to stay anonymous and prefer computer-mediated contacts, the online methodology[22] is the most adequate for carrying on research within this community. This methodology puts certain restrictions on the choice of research instruments. First, the instruments (e.g., tests, questionnaires) should not be familiar to the audience. Second, taking into account insecurity and expensiveness of the long-time access to the Internet, research is recommended to take a short time.

To measure flow, we used the questionnaire worked out and used by Hoffman and Novak.[16] It is not universally known in Russia, and it took only a short time.

The questionnaire was translated into Russian, shortened, administered within a smaller sample in both the offline and the online modes to adapt it to the Russian hackers' population. Specifically, we used a nine-item scale which measures flow as a combination of arousal, challenge, skill, control, exploratory behavior, play, interactivity, distortion of time, involvement. The flow, the telepresence, the

positive emotions and the focused attention items (used by Hoffman and Novak) were excluded. We found that the flow item provokes subjects to give universally positive answers, so the item was excluded as non-informative. Telepresense was excluded on the grounds that it is implied in the hackers' behavior itself, and the sample subjects reported the question being redundant. The focused attention was excluded since it is described as a consequence of the interactivity.[16] Positive emotions are usually believed to be a consequence of the play, so this item rarely appears in the flow questionnaires.[14,23]

Four-point Likert-type scales ranging from "strongly disagree" to "strongly agree" were used for responses. The scores might be summed up, the numerical result being the level of flow.

Measuring hackers' competence is a difficult task. Hackers themselves seem to have differing views on this specific sort of competence. Besides, hackers supposedly are only rarely universally competent; their skills in performing the preferred sorts of hacking behaviors might be much higher than their qualification in rarely/never performed hacking actions. Even selection of hackers from non-hackers is a very special task with differing views and criteria; neither selection of hackers nor practical measures of their competence can be developed within the grounds of psychological research.

Thus our subjects were self-reported, non-selected hackers. We take as granted that hackers need specific software and systematically visit special web-sites for hackers. We recruited visitors of these sites to participate in our research.

It is universally accepted that hackers differ in knowledge of the IT basics: most of the hackers' sources complain that some "newbies" (i.e., beginners) are active in primitive forms of hacking since they lack competence in the fundamentals of IT. Thus, instead of estimating the subjects' competence in hacking we inquired about their competence in computer use and IT-related experience. Namely, we inquired about their duration of computers & IT use (in years), and the variety of known software products and programming languages (in the number of pieces). Thus, competence was taken as a compound two-block measure of experience in the IT use.

Several questions were added to learn the Ss' demographic data (i.e., age) and geographical region.

Procedure

The questionnaire was administered as a web fillout form. It was posted on a personal homepage of one of the experimenters (O. Smyslova). After the questionnaire was placed on the web-page, subjects were solicited using online sources. The announcements and invitations to participate in the experiment were placed on the web-sites and web-pages containing special information for hackers. Two types of sources were used, evidently differing in the amount and quality of information—and with obviously differing audiences. The sources of the first type contain a wide range of software instruments for hacking, as well as general-purpose news and popular data about new books, music, etc. These sources are supposedly visited by somehow less competent hackers. The second type of sources contain much more sophisticated hacking instruments and only specialized news—these sources are supposedly visited by experts in hacking.

We realize that one cannot avoid some mixture in the composition of groups as a result of visits of expert hackers on less-specialized web-sites, and vice versa. Another sort of mixture might be the result of posting and cross-posting the announcements and invitations on some personal hackers' web-pages.

According to the two types of sources used to invite the subjects, the online survey period was divided into two periods: 25th of January to 25th of February (supposedly, the first group), and 26th of February to 18th of March, 2001 (supposedly, the second group). The results were handled using the statistical package Statistica.

RESULTS

Subjects' demography and computer use experience

All those who volunteered to participate in the research are self-selected subjects. A total of 457 subjects (215 in the first group and 242 in the second group) took part in the research. The average age was 23 years; 76% subjects of the first group and 85% of the second group were between 17 and 30 years old. Thus, the subjects were young, but mostly older than adolescents.

In the first group, 41.4% Ss reported they live outside Russia; the majority of the residents of Russia were Muskovites (17.7%). In the second group, 33.6% Ss reported they live outside Russia and 33.2% lived in Moscow. Many non-residents of Russia reside in the Ukraine and other republics of the former USSR; subjects from outside this geographical region are nevertheless numerous: 21.4% in the first group and 8.7% in the second group.

The procedural supposition that the two groups of subjects differ in competence seems to be correct. First, the average number of known software products is 3.9 (first group) and 5.2 (second group). Second, the over-5-years-experience in IT and in using software products is much more characteristic for the second group than for the first group: 81.8% of subjects versus 57.6%. The data show that, as we had supposed, in the second group the Ss are more competent.

The comparison of the groups of hackers

The discriminant analysis results. We used the discriminant analysis procedure with three variables: flow experience, duration of computer use and variety of known software products (the latter two stand jointly for competence). The forward stepwise method was used: the first variable extracted in the analysis was the flow variable, the next was the variety of the software products known and the least meaningful variable was the duration of the computer and IT experience.

The analysis of standardized coefficients of the canonical discriminant function (Table 1) makes it evident that the variable "Flow" is the major distinctive feature between the experimental groups.

The least competent in the IT hackers experience high level of flow. But hackers having average level of competence experience low level of flow. It is important to stress that the number of known software products is more important for the flow experience than the time duration of the use of computers and IT.

When tested the canonical discriminant function to predict the binary variable (group1/group2), the Wilks' Lambda was significant ($p < 0.0001$). Results show that the classification of Ss between the groups was good enough: 67.7% of correct classifications. Since the classification of over 30% of subjects was false, in the next section the results of inter-group classifications are presented.

TABLE 1. STANDARDIZED COEFFICIENTS FOR THE CANONICAL DISCRIMINANT FUNCTION

Variables	*Standardized coefficients of canonical function*
Flow	0.927901
The variety of known software products	−0.523860
The duration of computer use	−0.308284
Constant	0.184381

The cluster analysis. Cluster analysis using the *k*-means method was made to check inter-group classifications. This means that the formal criterion we used, namely Ss' visits to the highly specialized or, opposite, to the less specialized hackers' sources did not work for all the cases. The data presented in Figure 1 make it evident that the optimal classification divides our subjects into three clusters.

The following analysis is dealing with the way the subjects belonging to either of the two groups were classified into clusters. From Figure 2, we conclude that more than a half of group 1 Ss were referred to the first cluster. The rest of group 1 was almost equally (24% and 21%) distributed between the two other clusters.

Group 2 was less homogeneous, as is shown in Figure 3: while 48% subjects of this group belonged to the third cluster, 30% belonged to the first cluster and 22% to the second cluster.

Now we can return to the measures of flow and the two measures of the hacker's competence presented at the Figure 1. For the ease of analysis, the exact data are presented also at the Table 2.

The three clusters differ a lot. In cluster 1 the least competent Ss (in more details, with small number of known products and low duration of the use of computers and IT) experience high level of flow. In cluster 2 the highly competent Ss (with the highest variety of known software products, and the highest duration of computers and IT experience) report high level of flow. In cluster 3 the moderately competent Ss (in more detail, with moderate variety of known products and moderate duration of computers and IT use) experience very low level of flow. Thus, the moderately qualified Ss report a gap (a sort of a crisis) in the flow experience.

Post-experimental online interviewing. Post-experimental online interviews were undertaken to get more information about the role of the Ss' experience with computers and IT, their projects, processes of task choice while hacking. Additional questions were sent online to 30 subjects from each of the two groups, with data close to the centroids of the group. We got 37 replies (21 for the first group and 16 for the second). The most useful are the replies to the question on the specifics of task choice processes: the Ss reported two major mechanisms of task choice while hacking.

First we briefly discuss replies given by supposedly incompetent Ss who experience flow. For example, Serge (the first experimental group) wrote:

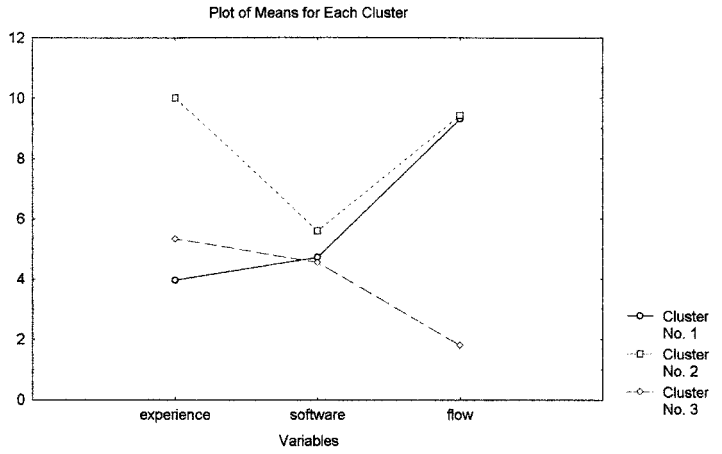

FIG. 1. Means for clusters of subjects.

"Actually, all the problems could be solved. I mean I can see the solution, all steps of it. But sometimes I have not enough experience with the software products I need for the project. If I choose the project to complete I try to estimate the time. Do I have time to learn new programs or not?"

Or M.G. (the first experimental group) wrote: "Big projects are not enjoyable for me. On a certain stage it becomes boring, because there is no result . . . Now I am doing only those projects, which I hope to complete quickly. Some time ago I did not understand why I was so interested in it, why it was so enjoyable to break the copy protection of software products . . . Later I understood that it was just fast results . . . It was faster than to complete my own project."

The task choice mechanism reported by Serge and M.G. might be called step by step choice. Possibly, this mode of task choice promotes precise matching of skills and challenges on every step, and thus the flow experience is maintained.

On the contrary, hackers who are supposedly highly competent and experience low level of flow choose their next tasks or projects within the hacking field according to their interests and do not coordinate it with the difficulty of the chosen task.

Here's the answer by Yuri (the second experimental group): "Everything depends on my temper and weather). Today I may want to work on free mail service (like www.mail.ru), tomorrow I may begin to create an accounting service for Linux. And the day after I would not do anything . . . Everything is up to me. Today it's interesting, tomorrow it's not."

As we can see from Yuri's words, he chooses the tasks by himself. Projects he mentioned are complicated enough; other programmers or teams have already developed some of them. The projects would take a lot of time and effort.

Y.K. (the second experimental group) says the same: "I always feel lack of knowledge, because I have a lot of ideas about different projects . . . and for realizing them I need a lot of information and knowledge. I choose only those projects which are interesting for me and don't pay attention on their complexity."

Two moments need to be stressed. First, the step-by-step task choice often leads to close correspondence of challenges of the task and of available skills, which is the mark of flow experience. And second, the task choice is regulated by intrinsic motives of cognitive nature, which lead to full involvement and engagement with the actual project. But if the task complexity overruns the available skills, actual motivation might be far from the flow experience.

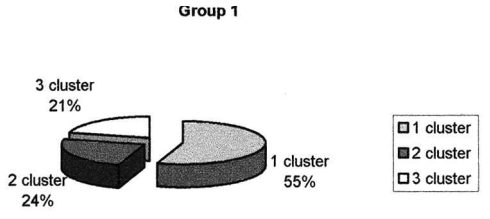

FIG. 2. The distribution of group 1 subjects into clusters.

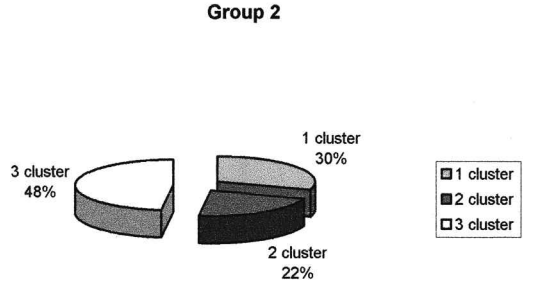

FIG. 3. The distribution of group 2 subjects into clusters.

TABLE 2. MEANS FOR THE THREE CLUSTERS

	Cluster 1 (181 subjects)	*Cluster 2 (109 subjects)*	*Cluster 3 (167 subjects)*
Experience in computer use (years)	4.0	10.0	5.3
Variety of known software products (pieces)	4.7	5.6	4.6
Flow	9.3	9.4	1.8

Conclusion on the hypothesis tested in the research. The results show that the hypothesis is wrong, since flow does not linearly increase with the increase of the hackers' competence. The relationship between hackers' experience and flow is more complicated than the straightforward correlation. Periods of flow experience are changed by periods of flow crisis and then by periods of flow renovation. In the post-experimental interviews the role of task choice in experiencing flow while hacking is revealed. These findings make it possible to construct and present a model of hackers' motivational development.

The model of computer hackers' motivation

We present a motivational model of hackers' development, which is based on the flow/non-flow ratio (Fig. 4). The major part of the model is in a good accordance with the results of our research (it is shown by solid arrows); a minor portion of the model is hypothetical and depends on non-empirical evidences (shown by dashed arrows). The model is based on a balance between the level of computer and IT (but not specifically hacking) skills and the level of challenges (or task choices) in hacking.

The mainstream of a hacker's development might be presented in the following way. An inexperienced hacker (a beginner, or a newbie) might find a matching combination of challenges and skills and start to experience flow. The flow motivation is strong, and the newbie feels comfortable. A hacker might stay at this stage for years; some evidences say that a great number of hackers are extremely inexperienced. To stay at a newbie stage means that neither skills nor challenges develop in a significant way.

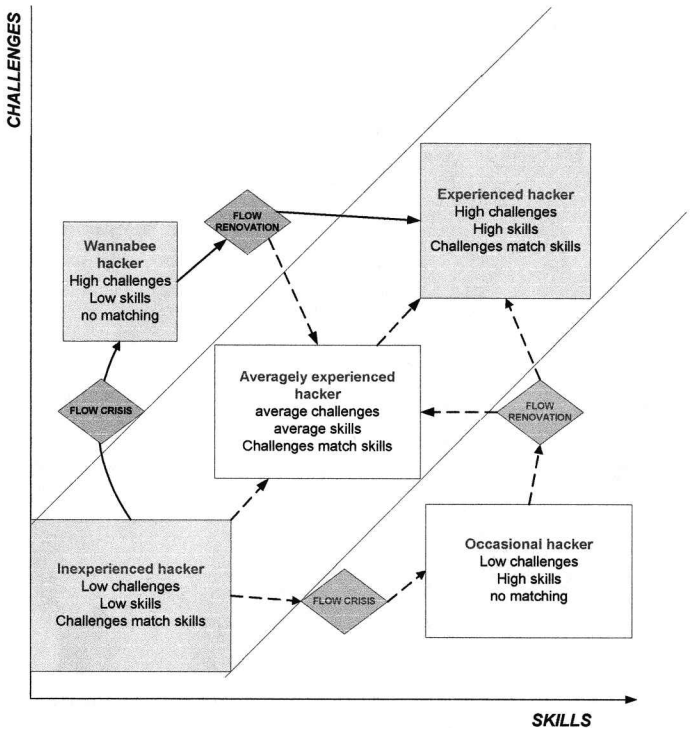

FIG. 4. Flow-based model of computer hackers' motivation.

In case a newbie hacker progresses, this might take place in at least three ways. The first is a step-by-step progress both in challenges and skills—first to an average and then to a highly experienced hacker—in such a way that challenges and skills keep matching at every developmental stage. Thus, the progressing hacker keeps experiencing flow all the time. The case of fine skills/challenges correspondence at every stage is probably rare, and hard to be recorded in a longitudinal study.

The two other ways of a newbie hacker progress mean, first, that a hacker gains new skills and lacks the correspondence of new skills to non-updated challenges. Or else a hacker takes high challenges and finds he/she lacks non-updated skills. Thus these two ways of a hacker's progress lead to periodical dropouts of the flow range, and the hacker periodically looses the flow experience. At the next stage the hacker might manage fine correspondence of skills and challenges anew and acquire the flow experience at a higher level of his/her progress in hacking. Constant matching of skills and challenges and non-interrupted flow seems to be a hard way of progressing.[22,24]

If an inexperienced hacker increases challenges, he/she turns to become a wannabee hacker, at least for a certain stage of his/her development. If the progress in skills lags behind the challenges, a hacker looses the balance of skills and challenges and thus looses the flow experience. Some evidence says that a hacker might stay at this stage long enough, trying to acquire prestigious goals and in fact never acquiring them. A wannabee hacker's rewards might lie in the social sphere: for example, he/she might boast in companies telling of their challenges and getting some social prestige. To renovate the flow experience, a wannabee hacker might either lessen challenges and to become an averagely competent hacker setting moderate challenges, or to update skills and to become a highly qualified hacker with challenges matching the available skills.

If an inexperienced hacker increases skills, he or she loses—at least temporarily—the fine matching of challenges and skills. His or her skills overrun his or her challenges until the challenges are not updated. When updated, the flow experience might come back at a higher level of skills/challenges correspondence. If the challenges are not updated, a hacker might turn into a qualified computer user or a programmer. Some evidences tell that former hackers turn into computer security officers; that means they loose motivation to pose high challenges in hacking (besides, they gain external motivation, e.g. good salaries). If a former hacker does not turn into a security expert, he/she might turn into an occasional hacker—one who puts high challenges on special occasions only. These occasions might consist in a revenge to a former employer, or to an ideological/political enemy (a hactivist action). Some evidences tell that former hackers might try to hack anew on special occasions, and—supposedly—to experience flow at a high level of skills/challenges balance.

In any case, progress in hackers' skills and challenges means a zigzag of the flow motivation development.

DISCUSSION

The hypothesis stated in research is not correct, since the relations between the flow motivation and hacker's competence did not turn to be as straightforward as it was hypothesized.

Hackers acquire a certain amount of software products in the very beginning of their career; later on their competence in applying the newest pieces of software might increase.

If not, they tend to reproduce their previously acquired skills, following instructions available in widespread manuals "how to hack (attack)." To increase competence might mean that new pieces of specialized hacking software are worked out and/or learnt. On this way now and then happen gaps between the available skills and the challenges. Some intermediate ways of developing one's competence in hacking are possible, too.

Computer/information security is nowadays restricted to modernization of security systems. The view is stressed recently that firewalls, crypto systems, etc. are not the only possible and needed way to increase security. It would be less expensive and no less effective to work out methodical guidance plus training courses in practical IT ethics (sometimes called cyberethics), and to distribute it broadly among tutors, teachers, and interested parents.[25] Classes in cyberethics might lessen the amount of both newcomers to the hackers' community, of evil hackers (so called crackers) and of the hackers' admirers.

It seems important to mention that developers of software products aim to facilitate the users' flow—if not while hacking, but in other types of human–computer interaction, especially in computer games and online communications. Specifically, user-friendly interfaces and universal standards make it easy for wannabees to learn programming step-by-step, choosing the next software product to be only a little bit more difficult than the previous

one. Developers of new technologies are aware of the theory of flow and are trying to apply it to Web design.[26]

CONCLUSION

The supposition that intrinsic motivation (specifically, flow) characterizes computer hackers' activity was empirically supported. The measures of flow are not consistent with our hypothesis: flow characterizes the least and the most competent hackers, and a period of a "flow crisis" in hackers' development is reported. This period is characteristic for those hackers who acquire moderate amount of competence. To get rid of this "crisis" and to start experiencing flow anew, hackers have to adopt an ambitious mode of task choice, i.e. to put before themselves problems irrespective of the likelihood of an easy and quick solution.

The results of the research have an evident heuristic value, since they help to state a number of new problems for discussion and for further research. The most important problems seem to be those that give new knowledge about the motivations of hackers, and about the motivational stages of their development.

REFERENCES

1. Turkle, S. (1984). *The second self: computers and the human spirit.* New York: Simon & Schuster.
2. Taylor, P. (2000). *Hackers. Crime in the digital sublime.* London: Routledge.
3. McGuire, S., D'Amico, E., Tomlinson, K., et al. (2002). Teenagers self-reported motivations for participating in computer crime. Presented at the 8th International Conference on Motivation, Moscow.
4. Weizenbaum, J. (1976). *Computer power and human reason. From judgment to calculation.* San Francisco: W.H. Freeman and Company.
5. Levi, S. (1984). *Hackers: heroes of the computer revolution.* New York: Bantam Doubleday Dell.
6. Sterling, B. (1992). *The hacker crackdown: law and disorder on the electronic frontier.* London: Penguin.
7. Ershov, A.P. (1972). Aesthetics and the human factors in programming. *Communications of the ACM* 15:501–505.
8. Knuth, D.E. (1974). Computer programming as an art. *Communications of the ACM.* 17:667–673.
9. The Jargon file, version 4.2.0, 31 Jan. 2000 [On-line]. Available: http://www.science.uva.nl/~mes/jargon/.
10. Denning, D. (1990). *Information warfare and security.* Reading: Addison-Wesley.
11. Hafner, K., & Markoff, J. (1995). *Cyberpunk: outlaws and hackers on the computer frontier.* New York: Simon and Schuster.
12. Rodgers, M. (1999). A new hackers' taxonomy [On-line]. Available: www.mts.net/~mkr/hacker.doc.
13. Deci, E.L., & Ryan, R.M. (1985). *Intrinsic motivation and self-determination in human behavior.* New York: Plenum Press.
14. Csikszentmihalyi, M. (2000). *Beyond boredom and anxiety: experiencing flow in work and play.* San-Francisco: Jossey-Bass.
15. Csikszentmihalyi, M. (1975). *Beyond boredom and anxiety: the experience of play in work and games.* San Francisco: Jossey-Bass.
16. Novak, T.P., & Hoffman, D.L. (1997). Measuring the flow experience among web users [On-line]. Available: http://ecommerce.vanderbilt.edu/ papers.html
17. Csikszentmihalyi, M. (1982). Toward a psychology of optimal experience. In: Wheeler, L. (ed.). *Review of personality and social psychology. 3.* Beverly Hills, CA: Sage, pp. 13–36.
18. Bishay, A. (1996). Teacher motivation and job satisfaction: a study employing experience sampling method [On-line]. Available: hcs.harvard.edu/~jus/0303/bishay.pdf.
19. Bryce, J., & Higgins, D. Optimal experience: a framework for understanding the phenomenology of computer use [On-line]. Available: www.uclan.ac.uk/facs/science/psychol/gcrf/recreat.htm.
20. Chen, H., Wigand, R., & Nilan, M. (1999). Optimal experience of web activities [On-line]. Available: http://web.syr.edu/~hchen04/conferencepaper/ExperiencesWeb.html.
21. Uekawa, K., Borman, K., & Lee, R. (2001). Assessing student engagement in mathematics and science classrooms using the experience sampling method [On-line]. Available: www.sistudyforum.org/pubs/5BormanUSI_1.pdf.
22. Trevino, L.K., & Webster, L. (1992). Flow in computer-mediated communication. *Communication Research* 19:539–573.
23. Whalen, S.P. (2001). Revisiting "the problem of match": contributions of flow theory to talent development. In: Colangelo, N., Assouline, S. (eds.). *Talent Development. IV.* Scottsdale, AZ: Great Potential Press, pp. 317–328.
24. Hoffman, D.L., Novak, T.P., & Duhachek, A. (2002). The influence of goal-directed and experimental activities on online flow experiences [On-line]. Available: www.ecommerce.vanderbilt.edu/research/manuscripts/index.htm.
25. McKenna, K., & Lee, S. (1995). A love affair with MUDS: flow and social interaction in multy-user dungeons [On-line]. Available: http://oak.eats.ohiou.edu/~sl302186/mud.htm.
26. Beveren, J.V. (2001). A conceptual model for hacker development and motivations [On-line]. *Journal of E-Business.* Available: www.ecob.iup.edu/jeb/December2001-issue/Beveren%20article2.pdf.

27. Voiskounsky, A.E., Babaeva, J.D., & Smyslova, O.V. (2000). Attitudes towards computer hacking in Russia. In: Thomas, D., and Loader, B.D. (eds.). *Cybercrime: law enforcement, security and surveillance in the information age.* New York: Routledge, pp. 56–84.
28. Birnbaum, M.H. (ed.). (2000). *Psychological experiments on the internet.* New York: Academic Press.
29. Repman, J., & Chan, T.S. (1998). *Flow in web based instructional activity: an exploratory research project.* Texas Tech University, Georgia Southern University.
30. Babaeva, J.D., & Voiskounsky, A.E. (2002). IT-giftedness in children and adolescents [On-line]. Available: http://ifets.ieee.org/periodical/vol_1_2002/babaeva. html, http://ifets.ieee.org/periodical/vol_1_2002/ babaeva.pdf.
31. Berkun, S. (2001). The role of flow in web design [On-line]. Available: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnhfact/html/ hfactor 10_1.asp).

Address reprint requests to:
Alexander E. Voiskounsky, Ph.D.
Psychology Department
Moscow Lomonosov State University
85 Mokhovaya str.
Moscow 103009, Russia

E-mail: vae-msu@mail.ru