УДК 343.9:004.738.5
DOI:https:doi.org//10.22182/ni.4112022.7
Прегледни рад

НАЦИОНАЛНИ ИНТЕРЕС
NATIONAL INTEREST
Година XVII, vol. 41
Број 1/2022
стр. 147-159

Ivana Luknar*
Institute for Political Studies, Belgrade, Republic of Serbia

SOCIAL CONTROL THEORY AND CYBERCRIME

Resume

The paper pays attention to the potential role that the social control theory has in the improvement and development of previous Information-Communication Technology (ICT) Policy. Online activities are daily routine of people all around the world. Emerging information and communication technologies create numerous challenges and issues how to regulate its use. ICT policy interests are closely related to concern of social order in cyberspace. The development of ICT possibilities at the same time follows development of new cybercrime forms. The ICT policy needs to explore new strategies and theoretical integration that transcend the existing criminological frame. The sociological theory of social control to a significant degree may predict and explain crime and how people define and respond to deviant behavior. How social control theory may order individual behavior in cyberspace? May it help prevention of cybercrime and maintain more safer and conscientious use of the internet? The following article provides an analysis of the possibilities of social control theory in maintaining the order in cyber society. Throughout the article, the social control theory is discussed by content analysis scientific method. Main purpose of the paper is to encourage concerning use of social control mechanisms as one of the effective tools for regulation in cyberspace and prevention of cybercrime.

Keywords: social control theory, ICT policy, cybercrime, cybersecurity, behavior.

* email: ivanaluknar@gmail.com

INTRODUCTION

The grow of ICT (Information and Communication Technology) had a profound impact on humankind's patterns in almost every field of social existence: business, government, the labor market, lifestyles etc. Internet and ICT appear as effective communication tools like never before during coronavirus world crisis. While, coronavirus health instructions encourage people all around the world to rely more than ever on ICT and social networks as recommended forms of communication, technological development and current coronavirus situation pushed ICT (Information and Communication Technology) forward in almost every field of our existence (Luknar 2020). Wide range of different reasons motivates people for using social network sites and to interact on ICT platforms; in order to stay in touch with: business partners and trends, family and friends (Joinson 2008; Smith 2011), current friends and to reconnect with old ones, others with shared hobbies or interests, to make new friends, find potential dating partners and follow celebrities, politicians or athletes (Smith, 2011) etc. The use of ICT facilities becoming an indispensable part of everyday life more and more widely used day by day. This reality leaving open the set of question of maintenance social control in cyberspace and online activities. Beside cyber security policies and measures (laws, protection and defense measures, etc) important part of prevention is indirect prevention. Part of the challenge for ICT users is their lack of comprehension of cyberspace, cyber threats, cyber frauds etc. The paper starts from a hypothesis: *through social control and education about proper/forbidden behavior and threats in cyberspace we may prevent or at least diminish cyber violations and cyber crime*. The purpose of the paper is to point to the importance of the indirect prevention of cybercrime and to encourage thinking about social control theory. Whether the concept of social control have the capacity to carry understanding of the importance of the conscientious behavior in cyberspace and provide indirect protection of cyber space and ICT consumers against a cyber violations? Article discusses the social control theory and its potential of cyber space regulation. Further, paper stimulates debate on how to ensure successful ICT/telecommunications regulation in a world of technological convergence.

First part of the paper deals with the issue of cybercrime, its various categories, opportunities of prosecution and recommendations for multilevel defense of cybercrime. Further, in the paper are presented the social control theory and possibilities of social control in prevention

of cybercrime and its implementation in ICT policy. Last part of the paper considering reconstituting of the subject through social control.

CYBERCRIME

Technological development and rapidly growing use of ICT contribute evolving criminal technigues. The term cybercrime refer to "traditional form of crime ... committed over electronic communication networks and information systems," the "publication of illegal content over electronic media," or any "crime unique to electronic networks" (Commission of the European Communities 2007). The terms "cybercrime", "computer crime", "computer related crime" or "high-tech crime" are synonymous often used interchangeably.

Cybercrime may involve a wide range of attacks that according to European Commission can be classified in three categories:

1. „crimes specific to the internet" such as attacks the integrity, authenticity, and confidentiality of information systems or phishing (e.g. fake bank websites, enabling access to victims' bank accounts etc)
2. "traditional" crimes such as fraud and forgery committed online
3. „illegal online content", including pornographic and child sexual abuse material, glorification of violence, terrorism, racism and xenophobia etc.

A cyber criminal may use many techniques to deceive victims. Considering transformative nature of the Internet and cybercrime, the label of cybercrime acts do not fall easily within the boundaries of the criminal law. There is, therefore, not always a legal basis for those type of crimes. Due to insufficient identification and reporting of cybercrime acts as well as difficulties of collection valid evidence for trial, there is a significant dark figure about this criminal acts. Experts agree that most cyber criminals are not caught; law percentage as 5% of all perpetrators are prosecuted (Kshetri 2009). I suggest eight "recommendations that can be taken to ensure multilevel defense of cybercrime":

1. Consciousness use of the internet;
2. Consciousness implementation of new digital technology
3. International monitoring, juridical cooperation
4. Multilevel transnational cooperation
5. Reducing dark number
6. Law enforcement responses
7. Improve cybercrime policing
8. Dedicated well trained police personnel (Luknar 2020, 624-626)

Online behavior and outcomes which feel instinctively wrong but do not give rise to criminal liability, may produce rise of new violent behavior in cyberspace. ICT policy governs how we use information and communication technology in almost every field of social existence. ICT policy also deals with the cyber safety and issue of cybercrime. Therefore, it is important to consider besides the direct ICT policy methods, the indirect methods of cybercrime prevention that may significantly affect behavior in cyberspace.

THE SOCIAL CONTROL THEORY AND ITS IMPLEMENTATION IN ICT POLICY

The social control theory implies a set of social measures, processes that encourage people to behave according to the law. The theory seeks to understand the ways moral codes, values, norms, commitments and beliefs reduces deviant behavior. The social control theory is closely related to the process of socialization and social learning. This concept has developed in two different directions. First direction is closely related to the primary group relations impact on individual behavior and second direction reffers to the impact of macrosocial institutions (education, religion, law and the political system).

Travis Hirschi (1969) has been shown that strenght of individual's bond to society was inversely related to delinquency involvement. "There are four elements of this social bond: (a) attachment to conventional others, such as parents and teachers; (b) commitment to conventional goals and activities, such as school; (c) involvement in conventional activities; and (d) belief in conventional norms. When these elements of the bond are weak, the individual becomes "free" to engage in delinquency" (Agnew 1991, 126). As Sutherland and Cressey mentioned: "inadequate socialization leads to amoral beliefs" (Sutherland & Cressey 1978, 81). Also, socialization by intimate others such peers may lead to delinquent behavior. Growing use of the Internet and ICT in education, everyday communication and leasure does expose youth's to online risks. Participation in online peer-to-peer communications and other activities may lead to potentially risky contacts, like cyberbullying and pornographic or aggressive images where youths are perpetrators, victims, or both. Initial social-psychological characteristics are important. As Williams mentioned: "Without emotions, social life, including our decision making capacities and our ability to make informed choices amongst a plurality of options, would be impossible" (Williams 1998, 761). But, human behavior doesn't rely so much on the emotions per

se; the social constructionism versus biology. Hochschild (1983) saw biologically derived emotion potentiality shaped by the social. Individual behavior is regulated in primary group relations, and various factors such as peers, school (Wiatrowsk 1978, 3), social class background (Wiatrowsk 1978, 96). As psychoanalytic sociologists (Richards 1989; Craib 1989; Elliott 1999) agree there is always a tension between outer and inner worlds, between social structure and society. The emergence of Internet and cyber space have bring a number of benefits, but also a tension between the real physical world and the online world and identity. The historical development of the concept of social control should keep up with technological development of worldwide society.

The work of Merton (1938) on anomie laid the fondation for a number of versions of social control theory. Merton presented a typology of modes of individual adaptation (Table 1), where innovation, ritualism, retreatism and rebellion represented major patterns of deviant behavior, with the exception of conformity.

Table 1. A typology of modes of individual adaptation (Merton 1938, 676)

	Cultural Goals	Institutionalized Means
Conformity	+	+
Innovation	+	-
Ritualism	-	+
Retreatism	-	-
Rebellion	+ -	+ -

+ = Acceptance; - - rejection; ~ = rejection of prevailing values and substitution of new values

First category, conformity involve persons who are satisfied with both cultural goals and accepted means for reaching these goals. In the second category innovation, Merton puts persons who adopted goals but using deviant or illegal means. The third category, ritualism involve those who lose sight of the cultural goals or cling blindly to the means to achieve goals which are not within their power. The fourth, retreatists are those who simply reject both the goals and the means of achieving them. The fifth category, rebellion involves those who reject the goals and means and who substitute and strongly strive for alternative illegitimate new pattern of social goals and means.

Beside basic psycho-social characteristics and modes od individual adaptation, structural arrangements may also lead to someones behaviour in real world as well as in online world. People

acting and making decisions that are shaped by large scale of structural arrangments. Johnson (Johnson 1991 in: Ulmer& Ulmer 2000, 317) mentioned threetype framework (Table 2) which focuses on situational opportunities and constraints. Each type corresponds to a distinct kind of situational definition in terms of a dialectic of constraint and desired choice. The framework further distinguishes between external and internal constraints.

Table 2. Threetype framework of commitment and their sources (Johnson 1991 in: Ulmer& Ulmer 2000, 317)

First type, structural commitment (external constraint):
1. Alternative lines of action: a. availability of alternatives b. relative attractiveness of available alternatives
2. Irretrievable investments
3. Difficulty of terminating lines of action once they are started
4. Social reactions to terminating lines of action once they are started
Second type, personal commitment (internal choice)
1. Attitudes toward lines of action
2. Attitudes toward others with whom one participates in lines of action
3. Definitions of self in terms of identities mobilized by lines of action
Thirdth type, moral commitment (internal constraint)
1. Sense of moral obligation to others with whom one participates in lines of action
2. Internalization of action-specific norms that discourage termination of specific lines of action once they are started
3. Internalization of general norms of consistency in lines of action

Information-communication technology has become an important facilitator to maintain and initiate social life, especially in the conditions of a covid-19 pandemic. Online interactions offer great potential for an individual regardless of age, gender or any other determinant from the physical (real) world by offering properties (rapid flow of information, content sharing, searching, etc.). But, the visibility of online posted content (text, pictures, video, audio, etc.) is potentially global and can be effortlessly copied and searched. The ease of remaining anonymous, fake profiles online can also trigger anti-social behavior. There are

different reasons for impersonating someone. For instance, to lure unsuspecting victims, to defame or to humiliate individuals as well as to catch predators. Some dramatic online incidents, leading to a criminal law response. According to above mentioned, cyber safety is one of the priority goals of the contemporary society which relies on technology and ICT.

Cyber safety is a turbulent arena, which constantly bring new risks and challenges. ICT policy should to combine the indirect methods such as social control with the direct active methods (procedures, strategies and legal system). At the same time there is need to foster persons' autonomy, of which risk-taking seems an inalienable part. The social control theory has potential to spread and share knowledge about cyberthreats, cybercrime, vulnerabilities and carry out raising awareness and determination to report cyber abuse authorities. This can be achieved by incorporating conscientious and responsible use of the internet and ICT into basic social values. ICT policy should find optimal balance between controlling that which is wrong cyber behavior and involves too high risks from the one side, and the freedom fit to human rights and essential opportunities of the Internet from the other side.

RECONSTITUTING OF THE SUBJECT THROUGH SOCIAL CONTROL

How to influence behavior of people in cyberspace? What theories about human nature and behavior may help? According to Freud's theory consciousness and unconscious psychological forces shape an individual's behavior. The poststructuralist and modern liberal approaches particularly focus on the relationship of subject and social structure. Both of the approaches poststructuralism and liberalism are discussed mainly through the work of the most influential theorists; poststructuralism through the work of Foucault, and liberalism mainly through the work of Giddens. These approaches in combination with the Marcuse's theory (Freudian-Marxist theory) offer an important dimension to understand human nature and behavior.

Freud's basic capacities of human nature that occur in his work are:

a) consciousness;
b) the potential to develop a social(ized) conscience;
c) rationality (instrumental but capable of development towards objectivity);
d) sex/aggression (which can be sublimated into, respectively,

love/idealism and work/competitiveness); and

e) the unconscious (seat of memories, dreams, fantasies and other processes fuelled by psychic energy). (Freud 1927)

Freud was fully aware that occurence of these basic capacities is influenced, formed and limited by society. He summed it up in two different and partly opposing principles:

- the pleasure principle by which the individual is driven to pursue gratification;

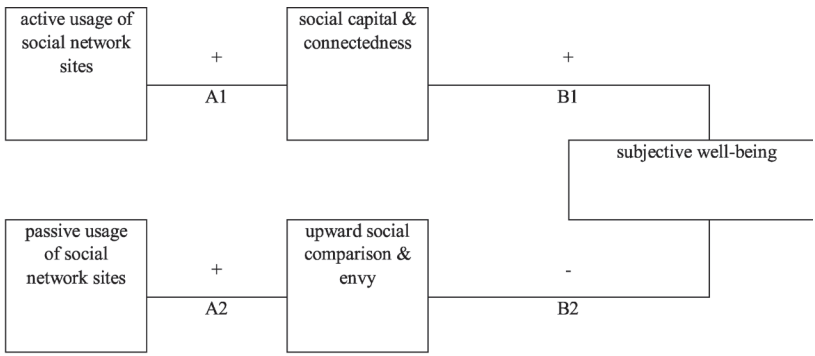
- the reality principle by which society (mainly through the regulation of work and reproduction) needs to direct and control the instinctual energies of individuals in a socially productive manner (Freud 1930, 308-314).

In explaining the human behavior, Freud relies on rationality. Weber (Weber in: Wolfgang 1992) brought out ideal type of social action and complemented the explanation of human behavior with motivation by reason, emotion, sentiment and self-interest. Therefore, if a person perceives cyber security as own interest and positively values it, the behavior of that person in cyber space will be satisfactory. Durkheim in his work was aware of the strength of human instincts, pointed to "the constitutional duality of human nature" (Durkheim in: Junge 2001, 106–7) which he believed society required firm moral and social control. Here we come to the point of necessity of social control. Foucault wrote of "points of resistance" as typically 'furrowing across individuals, cutting them up and remoulding them, marking off irreducible regions within them, in their bodies and minds" (Foucalt 1990, 96). As Nash mentioned the notion of resistance presumes some capacity to act against dominant forces (Nash 2000: 84). Frustration which derives from incomplete socialization may trensferred to the cyber domain. Giddens model of the the human psyche can be presented as three hierarchical mental capacities: discursive consciousness; practical consciousness; and the unconscious which are structured by potentially complex circumstance. "Values of the sanctity of human life, universal human rights, and the preservation of species and care for future as well as present generations of children may perhaps be arrived at defensively, but they are certainly not negative values. They imply ethics of individual and collective responsibility, which (as value claims) are able to override divisions of interest "(Giddens 1994, 20–21). In the worldwide growing dependence on information communication technologies, it is very important to positively evaluate cyber security. Deviant behavior is minimized, when a individual is relieved of a frustration. Marcuse sees potential for 'liberation' in the instincts or drives and emotions. His theory can be

summarized in two concepts: "the performance principle", was created as a result of long-term rationalization of domination. Those principle is "the prevailing historical form of the reality principle" (Marcuse 1969, 44). Growing specialization caused that person becomes more alienated from work. While, person works activities in the direction of socially useful performances that mostly do not meet their own needs and abilities, person becomes more alienated. Other principle "surplus repression" refers to "the restrictions necessitated by social domination" (Marcuse 1969, 44). "The occasional sacrifices involved in institutionalized conduct must be compensated by socialized reward" (Merton 1938, 674).

If cyber behave and cyber security are perceived as significant elements for humankind benefit, further development and use of ICT will lead to efficient ICT policy which provides safe utility for users. Verduyn et al. research (Verduyn et al. 2017) showed positive correlation between usage of social network sites and subjective well-being (Figure 1).

Figure1. The relation between social network sites and subjective well-being (Verduyn et al 2017, 284)



„Active usage of social network sites increases social capital and feelings of connectedness (path A1), which, in turn, positively impact subjective well-being (path B1). Passive usage of social network sites stimulates upward social comparisions and envy (path A2), which, in turn, negatively impact subjective well-being (path B2)" (Verduyn et al. 2017, 284)

Marcuse saw that the development of technology contribute to the qualitative change of human needs and act against the repressive use of energy as it reduces the time required to produce the necessities of life. Raising ICT awareness and consensus on certain universal ICT standards

and values, establishes guidelines and limits for ICT policy and action on national as well as global level. But it takes time to develop and expanded universal values from real world to online (virtual) world and to make consensus around them. Those values exist in some absolute, trans-historical sense, but they can be implement through multidirectional and dynamic social influence. If person perceive cyberspace and online behavior as well important as behavior in real space, person's approach to it will be conscientiously.

CONCLUSION

Emerging ICT trend is likely to affect the main regulatory issues, raising questions of how to deal with growing pressure to adopt a adequate policy regime. The need for a improvement of ICT policy is even more meaningful in new reality created by pandemic covid-19 when ICT innovations become the most powerful means of communication. Ultimately, the very boundaries and foundations of the overall ICT policy are expected to be contested by this technological momentum. In such dynamic conditions, the social control theory is imposed as a constant regulator of human behavior in cyberspace.

Governments around the world have struggled against cybercrime, made efforts to find best cyber defense and to harmonize the laws dealing with this issue. Those efforts should also include indirect techniques against cyber crime such is social control. Topic of the paper is the unique opportunity to study the social control theory's potential in prevention of cybercrime. The essence of the social control theory is that inadequate socialization leads to delinquent behavior. A social-psychological characteristics also can be the initial capsule for deviant behavior, which can also be reflected to behavior in cyberspace. Cybercrimes present several challenges for law enforcement. Historically, the greatest problem with pursuit and prosecution of cyber criminals has been technical, because the nature of those crimes. Technology development and ICT make easier everyday life, but also have consequence that traditional form of crime acts have a digital component. Prevention of cybercrime requires both direct and indirect means. First, direct means refer to the adequate cyber defense through key protection measures, policy, recognition and persecution of cyber threats and crimes. Second, social control should also apply to cyber behavior so it provides positive incentives for conformity to cyber roles and adherence to online (cyber) obligations as well as penalties (stigmatization). The wider context should always be kept in mind as technology's effects reflect active choices of

technology owners' perceived interests, existing organizational structures and routines, and by cultural norms. Social control have the capacity to carry a conscious understanding of the importance of the conscientious behavior in cyberspace and provide indirect protection of cyber space and ICT consumers against a cyber violations. So, it appears as possible mechanism of indirect cybercrime prevention. I see in the future the need for increasing cooperation and molding the ICT into the social matrix. The continuous development of information communication technologies requires that this issue be more effectively addressed.

REFERENCES

Agnew, Robert. 1991. „A longitudinal test of social control theory and delinquency." *Journal of research in crime and delinquency* 28 (2): 126-156.

Commission of the European Communities (2007). *Communication from the commission to the European Parliament, The Council and the Committee of the regions. Towards a general policy on the fight against cyber crime*. Brussels: Commission of the European Communities. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

Craib, I. 1989. *Psychoanalysis and Social Theory*. London: Harvester-Wheatsheaf.

Elliott, A. 1999. *Social Theory and Psychoanalysis in Transition: Self and Society from Freud to Kristeva* (2nd edn). London: Free Association Books.

Foucault, M. 1990. *The Care of the Self: The History of Sexuality: 3*. London: Penguin.

Freud, S. 1927. *Two Short Accounts of Psycho-analysis*. London: Penguin.

Freud, S. 1930. „Civilization and Its Discontents". In S. Freud, *Civilization, Society and Religion*. London: Penguin.

Giddens, A. 1994. *Beyond Left and Right: The Future of Radical Politics*. Cambridge: Polity.

Hirschi. Travis 1969. *Causes of Delinquency*. Berkeley, California: Universjty of California Press.

Hochschild, A. 1983. *The Managed Heart: Commercialization of Human Feeling*. Berkeley: University of California Press.

Joinson, A. N. 2008. "Looking at", "looking up" or "keeping up with" people? Motives and uses of Facebook. In: D. Gilmore (Ed.), *Proceedings of the 26th International Conference on Human*

Factors in Computing Systems (p. 1027–1036). New York, NY: ACM Press.

Junge, Matthias. 2001. „Zygmunt Bauman's Poisoned Gift of Morality." *British Journal of Sociology* 52(1): 105–119.

Kshetri, N. 2009. Positive externality, increasing returns, and the rise in cybercrime. *Communications of the Association for Computing Machinery* (*ACM)* 52(12): 141–144.

Luknar, Ivana. 2020. „Cybercrime – Emerging Issue". In: S. Jaćimovski (Ed.), „*Archibald Reiss Days*", Thematic Conference Proceedings of International Significance (Vol. 10, p. 621- 628). Beograd: Kriminalističko-policijski univerzitet.

Marcuse, H. 1968. *One Dimensional Man*. London: Sphere Books.

Merton, R. 1938. Social Structure and Anomie. *American Sociological Review, 3*(5): 672-682. doi:10.2307/2084686

Nash, K. 2000. „The "Cultural Turn", Social Theory: Towards a Theory of Cultural Politics". *Sociology* 35(1): 77–110.

Richards, B. 1989. *Images of Freud: Cultural Responses to Psychoanalysis*. London: Dent.

Smith, A. 2011. „Why Americans use social media friends". Accessed on August 7, 2021. http://www.pewinternet.org/2011/11/15/why-americans-use-social-media/.

Sutherland E.H. & Cressey D. R. 1978. *Criminology*, Philadelphia. J.B. Lippincott.

Ulmer T. J., & Ulmer T. J. 2000. Commitment, Deviance, and Social Control. *The Sociological Quarterly* 41 (3): 315-336.

Verduyn, P., Ybarra, O., Resibois, M., Jonides, J. & Kross, E. (2017). "Do Social Network Sites Enhance or Undermine Subjective Well-Being? A Critical Review". *Social Issues and Policy Review* 11 (1): 274—302.

Wiatrowsk D. Michael. 1978. *Social Control Theory and Delinquency*. Dissertations and Thesis. Paper 857. Portland State University: School of Urban Affairs. https://doi.org/10.15760/etd.857

Williams, S. 1998. „Modernity and the Emotions: Corporeal Reflections on the (Ir)rational'." *Sociology* 32(4): 747–769.

Wolfgang J. Mommsen. 1992. *The Political and Social Theory of Max Weber: Collected Essays*. University of Chicago Press.

Ивана Лукнар
Институт за политичке студије, Београд

ДРУШТВЕНА КОНТРОЛА И САЈБЕРКРИМИНАЛ

Резиме

Рад обраћа пажњу на потенцијалну улогу коју теорија друштвене контроле има у унапређењу и развоју досадашње политике према информационо-комуникационим технологијама (ИКТ). Активности на интернету су свакодневна рутина људи широм света. Растуће информационо-комуникационе технологије стварају бројне изазове и проблеме у вези са регулисањем њихове употребе. Интереси ИКТ политике су тесно повезани са питањем безбедности у сајбер простору. Истовремено са развојем ИКТ-а развијају се нове форме сајбер криминала. Политика ИКТ-а треба да истражи нове стратегије и теоријске интеграције које превазилазе постојећи криминолошки оквир. Социолошка теорија друштвене контроле у значајној мери може да предвиди и објасни злочин и начин на који људи дефинишу и реагују на девијантно понашање. Како теорија друштвене контроле може да уреди понашање појединца у сајбер простору? Може ли помоћи у превенцији сајбер криминала и одржавању безбедније и савесније употребе интернета? Чланак пружа анализу могућности које теорија друштвене контроле има у одржавању реда у сајбер друштву. У чланку се теорија друштвене контроле разматра употребом научне методе анализа садржаја. Основни сврха рада је да подстакне разматрање и примену механизама социјалне контроле као алата за ефикасну регулацију понашања у сајбер простору и превенцију од сајбер криминала.

Кључне речи: теорија друштвене контроле, ИКТ политика, сајберкриминал, сајбербезбедност, понашање.

* Овај рад је примљен 26. октобра 2021. године, а прихваћен на састанку Редакције 25. марта 2022. године.