



# ***Social Order and Network Security. Exploratory Research on TOR Hidden Network***

ROBERT STEFAŃSKI  
UNIWERSYTET ŁÓDZKI

## **Summary:**

As Internet becomes to grow outside of its physical carriers, it gains more influence over various subsystems constituting the social system in general. This manifestation is especially visible in the economical plane, in which a certain symbiotic relationship between the world wide network and other outernet institutions and organizations first occurred. With Internet becoming the modern central hub and a binder for various system components, it is safe to assume, that events taking place over the web, may or will have repercussions in the non-virtual reality. It is already valid to point out, that although the borderline between virtual and non-virtual realities is less and less visible, it may be sometimes required to artificially introduce this distinction. By presenting some of the possible actions that individuals may take while using hidden network services, an attempt shall be made, to determine what the possible outcome of the existence of such structures within the Internet may be from sociological perspective.

## **Key words:**

TOR, hidden network, social order, social security, system.

## Economical background for erosion of the borderline between the virtual and non-virtual reality

In its very beginning the global communication network was based on several different infrastructures such as EBONE, EuropaNET, NSFNET, ARPANET<sup>1</sup> and many others scattered around the world. These various networks were interconnected with each other after implementing TCP/IP<sup>2</sup>. It is crucial to point out, that the physical fundament allowing this merge was NSFNET's structure (Tanenbaum, 2003). NSF<sup>3</sup> was a nonprofit organization, which

charter forbid commercial application of its creation. At the same time it became clear that the maintenance cost of the physical grid is quite high. NSF coerced MERIT, ICM and IBM into creating a non-profit company called Advanced Network Services in 1990, which took NSFNET over, and therefore created a loophole allowing commercial use of Internet's resources (ibidem). As transactions made online became binding, it was required to implement certain legal regulations. Starting from this point the virtual and non-virtual realities began to merge on economical and normative planes.

With the commercialization of the medium, companies began to operate online. At the same time the increasing range of the Internet allowed more efficient use of advertisement. Additionally, based on income provided by the above, web providers are covering the cost of upkeep of the mediums infrastructure. This symbiotic relationship grows beyond the funding of the mediums physical carriers, as a huge variety of institutions are currently operating based or partially being based on internet resources. The newly formed integrated, electronical, global, realtime financial sector is a novelty (Castells, 2009) which not only emerged in its modern form after the marriage of the computer and telephone (Goban-Klas, 2006), but additionally has been made available to most of the population. The binding of the telephone and computer began with the creation of the second generation mobile devices, which was based on digital

technology<sup>4</sup>. With time it became possible to merge digital mobile phone with Internet by implementing WAP (Wireless Application Protocol) which resulted in the creation of the third generation mobile devices. As the technology standing behind the Internet, mobile phones, computers and transmission speed is developed at an improbable rate, the medium itself began to incorporate traditional media forms, just as every new technology absorbs and molds the old one. At the same time it is crucial to point out, that the new technology does not annihilate previous achievements, it rather adapts them, as the old one is still being used to fulfill the tasks for which the new one is either unsuitable or uneconomical (Bolter, 1990). And so, not only services, but additionally newspapers<sup>5</sup>, television, radio, social services, banking, shopping, cultural consumption and many more aspects of mankind's activities have been incorporated into Internet's structure and are now available on the screen of a device hidden in one's pocket. And yet all of these still do exist in its corporeal, non-digital, outernet form. The borderline between the virtual and non-virtual realities is more and more vague, as media, institutions, organizations, and even social movements are now functioning in these two parallel planes, which are constantly becoming more economically bounded.

## Internet as an extension of society

The term *system* refers in social sciences to an integrated whole, composed of various elements which are in a, more or less, equilibristic relation to one another. As an aggregate, this integrity needs to be clearly

separated from other systems (Sztompka, 2005). With the creation of the global communication grid and worldwide financial structure, the borderline between separate totalities began to erode (Giddens, 2004). Global communication network is however, as described previously, scattered and not coherent. Various regulations apply in different parts of the world to both the medium itself, as well as to its users. For example, for copyright infringement in Poland a user may be sentenced to jail, while in the USA pirates are required to pay a fine of even up to 150 000 USD per instance. The global system, although mosaic, is none the less total. It is the opinion of the author, the Internet due to incorporation of other media and by emerging into a form of global market, became a binding medium for various subsystems scattered around the world. Just like the global communication network is an extension for an individual's communicative and cognitive possibilities (McLuhan, 2004) the Internet may be considered, due to its transcendence, as a continuation of mankind and its organizational structure. By extending the collective consciousness, Internet became a slightly distorted reflection of existing outernet reality while becoming its adhesive<sup>6</sup>.

- 1 Advanced Research Projects Agency, currently called DARPA (Defence Advanced Research Projects Agency). [...] *The genesis of that mission and of DARPA itself dates to the launch of Sputnik in 1957, and a commitment by the United States that, from that time forward, it would be the initiator and not the victim of strategic technological surprises. Working with innovators inside and outside of government, DARPA has repeatedly delivered on that mission, transforming revolutionary concepts and even seeming impossibilities into practical capabilities. The ultimate results have included not only game-changing military capabilities such as precision weapons and stealth technology, but also such icons of modern civilian society such as the Internet, automated voice recognition and language translation, and Global Positioning System receivers small enough to embed in myriad consumer devices [...]* (Mission)
- 2 Transmission Control Protocol/Internet Protocol. A method of transmitting data between various networks. In the 70's there were several different transmission protocols in use, making some of the networks incompatible. NSF switched its network entirely to TCP/IP from the very beginning. Soon other networks did the same. The protocol is used and developed even today (Tanenbaum, 2003).
- 3 [...] *The National Science Foundation (NSF) is an independent federal agency created by Congress in 1950 "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense..." With an annual budget of \$7.3 billion (FY 2015), we are the funding*

*source for approximately 24 percent of all federally supported basic research conducted by America's colleges and universities. In many fields such as mathematics, computer science and the social sciences, NSF is the major source of federal backing (NSF at a Glance)*

- 4 In comparison to the first generation, which was based on analog technology.
- 5 Or maybe rather newsfeed.

- 6 The Internet considered as a medium cannot be treated as a reflection of modern society, due to various factors, out of which digital exclusion is the most important. The under representativeness of certain groups is however not that significant while analyzing the phenomena from systemic perspective, as the mosaicity of the metanetwork structure at least partially reflects economical potential of certain areas. This is due the diversity within the potential to invest in the physical network grid in the non-virtual reality. Considering the erosion of the borderline between virtual and non-virtual, on the economical plane certain areas may be theoretically identified with its networks.

The functionality and stability of every system, regardless of its kind, at a certain level of complexity needs to be maintained not only by informal but additionally by institutionalized forms of social control, which at least should be built based on a certain set of values functioning within the general population (Merton, 2002). Internet considered as a medium-type, binding system<sup>7</sup> on a global level, became a plane on which various activities of institutions, corporations, individuals and groups are being constantly monitored both informally, as well as by units designated to that particular task. These institutional forms of control are operating within the boundaries of a normative system, which needs to be codified and executed (Foucault, 2009) by comparing the existing factual state with the one considered as normatively perfect (Szenk, 2003), in order to ensure overall stability. Breaking or failing to comply with a certain set of rules, on a global or local level, may be interpreted as innovation, rebellion or withdrawal (Merton, 2002). As long as the scale of deviation is within the system's tolerance, the system itself will remain stable. If this scale is, however, large enough and the undertaken activities differ greatly from the acknowledged set of rules to the point of disobedience, it may cog the system's adaptive possibilities, leading to an overall structural failure (Szacki, 2002). As deviation is present in outernet reality, it

also manifests itself within the XXI century metanetwork.

### Introduction to hidden networks

It is true that Internet is not one coherent network, rather a network of networks, a metanetwork (Tanenbaum, 2003), which mosaicity was described in the first paragraph from the perspective of its physical carriers scattered around the globe. This frame of perception is however not fully comprehensive, as this particular feature of modern communications grid additionally manifests itself in its internal composition. Various networks may also be referring to different set of applications of the structures resources. And so satellite navigation, mobile grid, various local area networks, and finally hidden networks are all part of the enormous structure, that was referred to as *Internet* starting in the 80's (ibid).

Hidden network is an online structure functioning within the Internet and yet remaining inaccessible to most of the users due to various factors. Some are simply unaware of its existence, others do not know how to gain access to it. The most distinguished feature of hidden networks is that they remain mostly outside of the range of formal control. Due to implemented cryptographic mechanisms, it is impossible to track a particular individual over the web and submit him or her to a form of punishment for breaking the law, unlike in more formalized areas of the Internet.

An example of such a hidden network is TOR<sup>8</sup>, which protects its users anonymity by multiple layers of coding added to the data stream, and additionally rerouting the signal via various nodes. Data is being

transmitted simultaneously to all nodes within the network, where the decryption key is only in one of them. After stripping the first layer of coding, the data is being transmitted again on the same basis until it reaches the designated server. Response is being transmitted based on the same principal.

### Investigating TOR – methodological outline

As TOR's main goal is to maintain its users anonymity over the web, they were more than unwilling to participate in any kind of research. This attitude arouses some suspicion. What content lies within? Why are some of the Internet users starting to migrate to hidden networks? And finally, can their actions possibly distort widely understood social order? Although a particular individual using TOR cannot be pinpointed over the web<sup>9</sup>, the content of TOR pages can be accessed and analyzed. Based on that content an attempt has been made to recreate one's possible actions, which were later on compared with the existing polish normative system. By fulfilling this task it was possible to declare, whether the page's content needed to be considered illegal, and additionally it allowed to approximately determine if a user could be designated as a criminal, under certain circumstances.

At this point it is valid to point out several weaknesses of this method. Internet is a global structure and it may seem that referring to polish regulations is at least inadequate. It is however valid to point

out that criminal acts, with the exception of war crimes, are no subject of interest to international law, as it mostly refers to local regulations (Królikowski, Wiliński i Izydorczyk, 2008). Nevertheless, some acts shall be condemned as similar on a moral basis, regardless of the legal system used for analysis.

As TOR cryptography voids using any kind of search engine, there is no full index of its content. It was possible to find certain pages thanks to parasites, containing links to other TOR sites. These links were provided with a short description, however most of them was out of date. Guessing a page name was also not possible, as TOR addresses are a chain of random letters, digits and marks ending with the suffix .onion. Therefore, no representativeness is to occur on any level.

Recreating possible users activities based on the pages content, was intended to remain within the possible virtual borders. However as Internet already reaches beyond its physical carriers, it was sometimes required to exceed beyond the strictly virtual reality, and anticipate actions that may occur in the real world. Nevertheless, these hypothetical actions were composed in an attempt to fulfill a process that began online, and assuming that an individual will try to complete what he has started.

Additionally there is no way to prove that the pages found within the TOR network are in fact real. A metaphor may be used, in which we are whispering to someone in a dark room, and he answers the same way. We know we are communicating, but we don't know with whom. Also it is crucial to point out, that the research was finalized in June 2014, and some of the material may be out of date. Due to these limitations, the data gathered should be treated rather as an artifact and analyzed with caution.

<sup>7</sup> Or rather subsystem depending on the perspective. Assuming that the erosion of the borderline between virtual and non-virtual is complete, the newly developed global structure which is a total system, can be identified with the Internet itself. If this erosion is however not fulfilled, Internet can be considered only as a subsystem, while the system itself remains above.

<sup>8</sup> The Onion Router, a multiplatform anonimous network, first released on 13th of September 2003.

<sup>9</sup> For as long as the cryptographic mechanisms remains unsolved, and for as long as the individual is implementing all of the required security measures.

## Characteristics of selected TOR sites

In total fifty different TOR sites have been analyzed. They allowed the user to: purchase firearms, stolen goods or goods from an unknown source, fraud documents and currency, commissioning murder or virtual attack, money laundering or viewing child pornography. Aside from content and services that seem illegal at first sight, there are many sites offering fully legal and accepted services, such as forums, online hosting or e-mail services.

Within the TOR network two search engines exist, however using that term to describe these services is at least an overstatement. DuckDuckGo allows browsing the *formalized* areas of the Internet from within the TOR network, voiding the possibility to gather any user metadata and prohibiting tracking ones actions over the web. This service is however not capable of running a search within the TOR network itself. TORCH<sup>10</sup> on the other hand allows searching within the TOR network, it is however very inaccurate. At the time of conducting the research its effectiveness varied between 0,05% and 5%<sup>11</sup>. At this point it is valid to underline the existence of parasites, which contain links to other pages, provided with a short description of the content to be found. These sites allowed the research to continue as they were functioning as an equivalent to search engines. Although TOR network is quite rudimental due to its mechanics<sup>12</sup>, it is

possible to create an IRC<sup>13</sup> based social-like portal, where users have the possibility to interact directly with one another. They can add content to their own tab, however it is being automatically deleted after the user logs out. One of the most common utilities available within TOR network are bitcoin services. Bitcoin is a kind of virtual currency used for paying for various goods. The service provider usually requires a commission, which at the time of conducting the research was mostly 1% of the transactions value. Appointing a 3rd party to handle bitcoin transactions on one's behalf allows to widen the possibilities of these TOR users, that have insufficient knowledge to operate the virtual currency themselves. It is valid to point out that bitcoin is not subjected to polish regulations. It can be however exchanged into "real world" currency (mostly USD). Additionally standardized TorShops began to appear, which basically are a template allowing to exchange one's services or goods for bitcoins. It is valid to point out that the virtual currency is not characteristic only to hidden networks, but it additionally functions in non-hidden networks as well. Within the TOR network we can also encounter services that do not exist or are at least are not heard of in the non-hidden areas of the Internet, such as communication form for The New Yorker Magazine. It is a standard communication window, that one can use to send information to the editorial office, without the fear of being tracked over the web. Another kind of such a service is pastethis.i2p, thanks to which a user can send a short message to a particular IP address in a form of a web pop out. After reading it, the content vanishes

permanently. There are also pages available, which are committed only to developing the TOR project. Within their content one may find additional tips on how to stay hidden within the Internet.

One of the most drastic content that is to be found within the TOR network are pictures and films with child pornography. Children are caught during sexual acts with their equals, as well as adults of both genders. Although producing such content, storing it or disseminating it in any form is strictly forbidden, things get a little more complicated when it comes down to analyzing the actions of the user. As per polish regulations storing this data in any kind of form is strictly forbidden. Legislator left room for no exceptions, including expert witnesses or prosecutor. As the data is being temporally stored within random access memory files, the user would commit a crime by default, even if he encountered such content unwillingly and by accident (Siwicki, 2011). It is however an informal practice to not punish the users who do not store such files on their hard drives or in other permanent forms (Verdict, 2012). This finds support in the opinion of Marek Mozgawa in his commentary to the article 202 of the penal code, who describes storing such or other data as [...] *saving certain content on an adequate, corporeal carrier e.g. CDs or magnetic tapes*<sup>14</sup> (Mozgawa, 2013). On the other hand there are pages functioning within TOR hidden network, that present pictures with nude children. These pictures, although sometimes posed, present no sexual act or other form of sexual content. Children are shown while playing naked in the yard or while being on a nudist beach. As characteristics of the paragraph 202 of penal code are

not fulfilled in this situation, I am forced to label this content as legal, even though a possibility of sexual stimulation exist for certain individuals. The last kind of activity that needs to be described while presenting child pornography within TOR network is a forum in which its users presented a huge variety of threads. Users exchanged fictional sex stories, described their real experiences related to sexual activities with children, they gave each other tips on how to avoid being caught by the authorities, how to lure children or how to dispose of a body. In relation to the article 18 paragraph 3 of the penal code such statements can be considered as aiding and abetting. Two things are crucial to point out, namely that such an aid needs to occur before or while the actual crime is committed and that no particular person needs to be addressed in order for the aid to be considered as guilty, since the phrase [...] *who with intent that another person commits a criminal act*<sup>15</sup> does not impose such requirements. At the same time there was a thread present, in which the participants of the conversation admitted among themselves, that they are aware of their "illness", and they exchanged ideas on how to avoid abusing children. Among presented ideas one could find propositions varying from solitude to chemical castration. Although not every thread may be considered as illegal, the forum as a whole needs to be labeled as functioning against polish legal system.

It is common in the TOR hidden network to create scattered wiki pages. These are generally slowly merging to become an alternative to officially functioning Wikipedia. Their content for each article is however

<sup>10</sup> The Onion Router Search Engine.

<sup>11</sup> As per description provided at the time of research available within TOR.

<sup>12</sup> Due to implemented cryptography the transmission speed is limited, which results in TOR looking more like Internet from the late 80's.

<sup>13</sup> Internet Relay Chat – application allowing to transfer messages in form of text between groups or individuals that are connected at the time.

<sup>14</sup> Free translation

<sup>15</sup> Free translation from article 18 of the polish penal code.

much more extensive. For example under the phrase *amphetamine* in addition to information available in the official online encyclopedia, we will find links to distributors operating within hidden network, methods of home production and a list of suppliers offering required compounds.

Among some files available under certain links one can find for example a very interesting cookbook. The file contains approximately 600 recipes for breaking locks, creating homemade pipe bombs, traps, firearms and basic medicine. The file is basically a guerilla warfare manual. Another file is for example .50cal which is a manual for creating a .50 caliber sniper rifle using home power tools available in the local market. The content in this case is however fully legitimate. Nevertheless, creating such firearms in the real world is not.

Another peculiar thing that takes place in the hidden network is the possibility to purchase certain goods, that are or will be stolen for the buyer and sold for about half of the market price. This aspect requires no further explanation. However what if the source of these goods are unknown to the buyer? As per article 292 paragraph 1 of the penal code, [...] *who based on the circumstances may believe that certain goods were obtained illegally, purchases, helps to sell, accepts or helps to hide these goods, may be sentenced up to 2 years of prison*<sup>16</sup>.

Among other pages that have been encountered and labeled as illegal, one can find sites allowing, purchase of firearms and drugs with international shipping, money laundering, commissioning on-line attacks on 3rd party servers, and finally commissioning murder. Purchasing a firearm (presumably used as serial numbers on the side were wiped) or drugs is quite

easy in the TOR network. One needs only to setup his bitcoin account, gather enough funds and pay by pasting a link to part of his virtual assets into the sellers page. Bitcoin can be mined by using various technics or purchased from a broker. At the time of conducting the research a used handgun was available for a virtual equivalent of less than 7 GBP. Ammunition was also available. What is most interesting, is that international shipping within The European Union was available for an additional fee of approximately 50 GBP<sup>17</sup>. Online drug stores selling marihuana, amphetamine and other substances were operating mostly in the USA, with no possibility to ship the requested merchandise outside of the US. It is however safe to assume that equivalents of such sites do exist for other markets around the globe. A cyber-attack on particular individual was available starting from 100 USD. The same kind of attack but against a corporate server was available starting from 350 USD. Commissioning an assassination was available via a website called The Hitman Network, starting from 10 000 USD. The service provider declined assassinating children and influential politicians. Service was available in the US, Canada and European Union. Purchasing illegal merchandise such as firearms and drugs is not prohibited itself. Nevertheless, possession of these items is. In order to prosecute individuals making such a purchase a different legal construction needs to be used. Following the article 13 paragraph 1 in relation to the article 263 paragraph 2 of the penal code (for firearms) and in relation to article 58 paragraph 1 of

<sup>17</sup> These values may have been slightly different, however the author is more than sure that purchasing a handgun at that time would cost no more than 55–60 GBP in total, shipping included.

the Act on Counteracting Drug Addiction<sup>18</sup> in the case of illegal psychoactive substances, attempting possession can be and is in fact treated as a crime. Commissioning assassination creates even more possible legal scenarios. Needless to say, that is due to the mechanics of the contract being sealed, where the service provider would contact his employer within a certain time after receiving payment, it is possible to withdraw from the entire affair, until providing details of the target. Up to this point it is safe to assume that no crime occurs on the side of the employer. After providing such details, the contract is however sealed and therefore a crime is committed.

Last possible activity encountered over the TOR network was the potentiality to purchase forged money or documents. Possession of these items is not a crime for as long as there is no intention to use them. Creating such items is however illegal. Again a legal construction using article 18 paragraph 3 of the penal code would need to be used in order to prosecute such individuals.

### Summary of the TOR exploration

During the research, twenty-four TOR sites have been labeled as functioning against polish regulations. Only in 15 cases possible user's activities have been classified as illegal. This means that two possible scenarios exist, in which the content of a page is unwarranted, and yet one does not commit a crime by merely using the site, and that although the content is prohibited, one's actions are legal to a certain degree. In this case the motive behind hiding ones identity within TOR is quite obvious. But what about the other 26 pages, where both the content and users activity cannot be

<sup>18</sup> Free translation

classified as illegal from any perspective? During the research conducted for the purpose of authors thesis, certain aspects of the hidden network were compared with their counterpart from the official areas of the Internet. Outside of the hidden network most users are following a certain set of rules that are almost always described in the terms of use of the particular page. Why do people abide these set of rules, if most of them never read the terms of use? In the authors opinion it is a manifestation of conformism brought from outside of the web. As the regulation functioning within a non TOR web portal are merely an adaptation of functioning law, which is, or at least should be, based on a set of values functioning within the population, one knows these rules instinctively. But why to follow these set of norms while within the web? Following Erving Goffman, an individual may go by a certain pattern of behavior, even if he does not necessarily accept it. This is because one is convinced that he is being watched by an invisible audience, that has the power to enforce the expected behavior if required (Goffman, 1981 following: Szacka, 2003). This would suggest that users either do not feel anonymous over the Internet, or that they have internalized the norms. The first explanation finds application in analyzing the behavior of TOR users who do not exceed the boundaries set by the society in the form of widely defined normative system.

### Hidden networks – are they a threat?

As the borderline between outernet and internet reality erodes on several planes, every aspect of this bondage would need to be taken into account separately. On the economical plane there are various threats

<sup>16</sup> Free translation

to modern social order, such as viruses which may lead to distortion of the cash flow between various markets based on Internet. Using bitcoin as a currency additionally influences the economical plane, as it is impossible (at least for the time being) to pay digital taxes. Cracking and commissioned online attacks may lead to disruption of the world's communications network. Piracy influences incomes for artists and corporations, hyper-discourses taking place via Internet have impact on general views and perception of reality. All of this seems however less relevant than the possibility for a certain group of people or organizations to coordinate their actions over the web without any form of social control, regardless whether formal or informal.

Society from systemic perspective is based on various smaller subsystems, such as economical, political, legal or any other. These subsystems are required to adapt to possible changes, as they are constituting the society in its specific aspects. Each of these subsystems has a certain goal, that needs to be achieved in order to create overall stability. This can however only be done, if every individual, group and organization is subjected to the same set of rules created by the legislator (Hobbes, 1651). Executing these legal requirements with the aid of legal system has various functions, such as educational, disincentive, therapeutic and many more including reinforcing the opinion that the system is capable of maintaining order (Foucault, 2009). Without ensuring punishment for crime, the entire system based on compliance is sure to collapse. And yet a group of people remain (on a virtual plane and into certain extent) outside of the systemic grasp. Of course their actions are limited, and it remains possible to implement negative sanctions upon apprehending them in

the outernet reality. Nevertheless, as long as these groups are operating within hidden networks, tracking them down by law enforcement is more than unlikely, as even if their actions sometimes may require to operate in the outernet reality, it is still necessary for the authorities to be aware of certain events. As long as they remain outside of formal control, they are undermining social order.

On the other hand, migration to hidden network can be interpreted as a form of escaping from legal limitations. This would suggest that people are losing faith into the legislators capabilities in general. Again this can be considered as a threat to the system, as authority's position is being undermined by these users.

Perhaps total transparency, which can be obtained by further anchoring the reality into Internet, is the answer to the threats created by modern society? Another question remains unanswered: can man's internal will to dominate over other beings be overcome, allowing the creation of such transparent society, where social control would not be monopolized but evenly distributed among the citizens? 🙄

**Robert Stefański** – mgr, jest absolwentem Instytutu Neofilologii i Komunikacji Społecznej Politechniki Koszalińskiej. W 2014 roku uzyskał tytuł magistra w Instytucie Socjologii Wydziału Ekonomiczno-Socjologicznego Uniwersytetu Łódzkiego. Obecnie jest doktorantem w Katedrze Socjologii Polityki i Moralności Instytutu Socjologii Uniwersytetu Łódzkiego. W toku swojej działalności naukowej koncentruje się na roli nowych mediów i globalnych struktur informatycznych w kształtowaniu nowego porządku społecznego.

**Afiliacja Autora:**

Katedra Socjologii Polityki i Moralności, Instytut Socjologii, Wydział Ekonomiczno-Socjologiczny, Uniwersytet Łódzki  
E-mail: [stefanski.robort@gmail.com](mailto:stefanski.robort@gmail.com)

## Bibliography:

- Verdict, II AKa 171/12 (Appeal Court in Wrocław September 27, 2012).
- Bolter, D. (1990). *Człowiek Turinga*. Warszawa: Państwowy Instytut Wydawniczy.
- Castells, M. (2009). *Koniec tysiąclecia*. Warszawa: PWN.
- Foucault, M. (2009). *Nadzorować i karać. Narodziny więzienia*. Warszawa: ALETHEIA.
- Giddens, A. (2004). *Socjologia*. Warszawa: PWN.
- Goban-Klas, T. (2006). *Cywilizacja medialna. Narodziny nowego społeczeństwa*. In L. H. Haber, & M. Niezgoda, *Społeczeństwo Informacyjne. Aspekty funkcjonalne i dysfunkcjonalne*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.
- Hobbes, T. (1651). *Lewiatan*. Retrieved March 28, 2015, from XV Liceum Ogólnokształcące w Bydgoszczy: <http://ftp.liceumxv.edu.pl/historia/PDF/Hobbes.pdf>
- Królikowski, M., Wiliński, P., & Izydorzycy, J. (2008). *Podstawy prawa karnego międzynarodowego*. Warszawa: Wolters Kluwer.
- McLuhan, M. (2004). *Zrozumieć media. Przedłużenie człowieka*. Warszawa: Wydawnictwa Naukowo-Techniczne.
- Merton, R. (2002). *Teoria socjologiczna i struktura społeczna*. Warszawa: PWN.
- Mozgawa, M. (2013). Komentarz do art. 202 k.k. In M. Mozgawa, M. Budyn-Kulik, & P. Kozłowska-Kalisz, *Kodeks karny. Praktyczny komentarz*. Warszawa: Wolters Kluwer.
- Mission. (n.d.). *Defence Advanced Research Projects Agency*. Retrieved June 7, 2015; from Defence Advanced Research Projects Agency: <http://www.darpa.mil/about-us/mission>
- NSF at a Glance. (n.d.). Retrieved March 28, 2015, from National Science Foundation: <http://www.nsf.gov/about/glance.jsp>
- Siwicki, M. (2011). Posiadanie pornografii dziecięcej. In *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne*. Warszawa: Wolters Kluwer.
- Szacka, B. (2003). *Wprowadzenie do socjologii*. Warszawa: OFICYNA – W” Naukowa.
- Szacki, J. (2002). *Historia myśli socjologicznej*. Warszawa: PWN.
- Szenk, J. (2003). *Kontrola społeczna jako proces samoregulujący. Teoria i badania socjologiczne*. Tyczyn: WSSG.
- Sztompka, P. (2005). *Socjologia zmian społecznych*. Kraków: ZNAK.
- Tanenbaum, A. (2003). *Sieci komputerowe, Kompendium wiedzy na temat współczesnych sieci komputerowych*. Gliwice: Helion.

## Cytowanie:

Stefański Robert, (2015), *Social Order and Network Security. Exploratory Research on TOR Hidden Network*, „Władza Sądzenia”, nr 5, s. 113–124 [dostęp dzień, miesiąc, rok]. Dostępny na [www.wladzasadzenia.pl](http://www.wladzasadzenia.pl).

## **Porządek społeczny a bezpieczeństwo sieciowe. Badanie eksploracyjne sieci ukrytej TOR**

### **Podsumowanie:**

Wraz z rozwojem, Internet zaczął wykraczać poza swoje fizyczne nośniki, obejmując zasięgiem kolejne podsystemy konstytuujące system społeczny. Jest to szczególnie widoczne w płaszczyźnie ekonomicznej, w której po raz pierwszy zaistniała symbiotyczna relacja między siecią, a instytucjami i organizacjami poza sieciowymi. Ponieważ Internet, który stał się swoistym centrum, a jednocześnie spoiwem dla poszczególnych elementów składowych społeczeństwa, wykracza poza rzeczywistość wirtualną, zasadnym staje się przypuszczenie, że zdarzenia mające miejsce w sieci również znajdą swoje odzwierciedlenie w rzeczywistości poza cyfrowej. Należy jednocześnie zauważyć, że rozróżnienie na rzeczywistość cyfrową i poza wirtualną jest obecnie bezzasadne, niemniej może być miejscami konieczne. Poprzez zestawienie możliwych działań jednostek w ramach sieci ukrytych, podjęta zostanie próba określenia możliwych skutków istnienia takich struktur w ramach Internetu z perspektywy socjologicznej.

**Słowa kluczowe:** TOR, sieci ukryte, porządek społeczny, bezpieczeństwo, system.