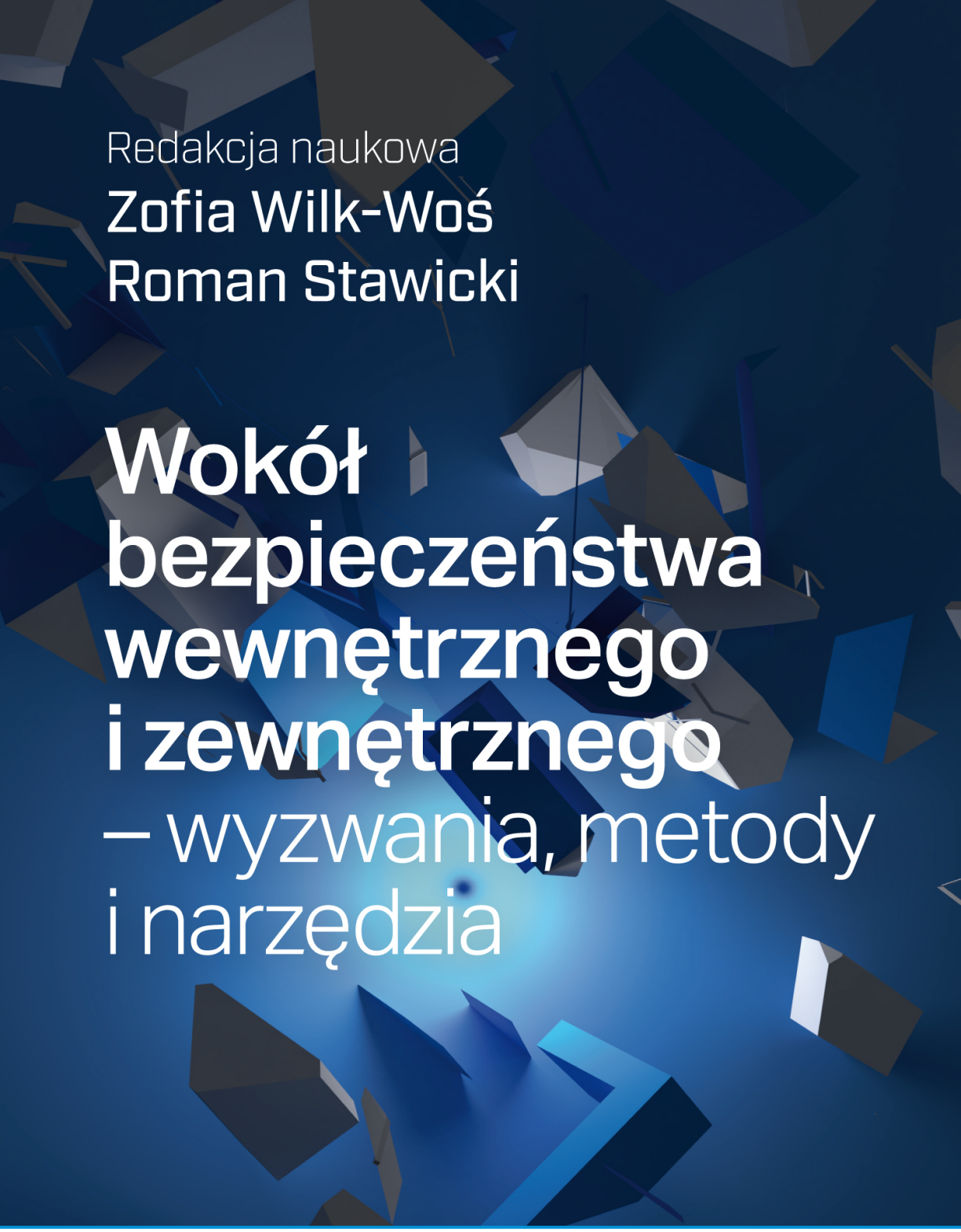


Redakcja naukowa

Zofia Wilk-Woś

Roman Stawicki

Wokół bezpieczeństwa wewnętrznego i zewnętrznego – wyzwania, metody i narzędzia

Nr 91

Studia i Monografie

Łódź-Warszawa 2019

Społeczna Akademia Nauk Łódź

Redakcja naukowa
Zofia Wilk-Woś
Roman Stawicki

Wokół bezpieczeństwa wewnętrznego i zewnętrznego – wyzwania, metody i narzędzia

Nr 91
Studia i Monografie
Łódź-Warszawa 2019

Społeczna Akademia Nauk
Łódź

Monografia recenzowana
Recenzenci: Jarosław Ropęga, Mirosław Kwieciński

Redakcja naukowa: Zofia Wilk-Woś, Roman Stawicki

Korekta językowa: Małgorzata Pająk, Agnieszka Śliz, Dominika Świech

Skład i łamanie: Małgorzata Pająk
Projekt okładki: Marcin Szadkowski

Studia i Monografie nr 91
2019

ISBN: 978-83-64971-61-7

Wydawnictwo Społecznej Akademii Nauk
Kilińskiego 109
90-011 Łódź
tel. (42) 664 22 39
(42) 676 25 29 w. 339

Spis treści

Wstęp

Do rąk Czytelników oddajemy pierwszą z nowej serii monografii poświęconych zagadnieniom bezpieczeństwa i zarządzania kryzysowego, przygotowanych przez Instytut Bezpieczeństwa Narodowego Społecznej Akademii Nauk w Łodzi.

Publikacja składa się z ośmiu części pokazujących wieloaspektowość wyzwań w obszarze bezpieczeństwa i zarządzania kryzysowego. Monografię rozpoczyna rozdział odnoszący się do niezwykle aktualnych i coraz szerzej poruszanych w badaniach naukowych kwestii cyberbezpieczeństwa i cyberzagrożeń. Autorzy zwracają naszą uwagę na nieustanną walkę w Internecie między tymi, którzy chcieliby śledzić działania jego użytkowników, a tymi, którzy wierzą w anonimowość. Podkreślają oni, że ostatnia debata „Right to be forgotten" („Prawo do bycia zapomnianym") pokazała, że bardzo niewiele można ukryć w Internecie, a usunięcie tych śladów może być trudne. Z drugiej strony Internet jest również miejscem, w którym dzięki anonimowości przestępczość może się swobodnie rozwijać. Obok bezpieczeństwa w Sieci kolejnym istotnym zagadnieniem dla większości ludzi jest bezpieczeństwo w środowisku szkolnym. Wszyscy jesteśmy bowiem zainteresowani zapewnieniem naszym dzieciom bezpieczeństwa w szkole. Problemom zagrożeń w środowisku szkolnym poświęcona jest kolejna część monografii, w której wskazano czynniki mogące obniżyć poziom ewentualnych zagrożeń i wpłynąć na wzrost bezpieczeństwa uczniów.

Następna część publikacji dotyczy problematyki zarządzania kryzysowego. Przedstawiono w niej propozycję struktury repozytorium dobrych praktyk, które będzie można zastosować w publicznym zarządzaniu kryzysowym. W ramach opracowania Autorzy określili strukturę repozytorium dobrych praktyk, zaproponowali przykład charakterystyki metody według wzorca zaimplementowanego w repozytorium oraz rekomendacje technologii wykonania repozytorium.

Jedną z istotnych dla współczesnego bezpieczeństwa dziedzin jest bezpieczeństwo ekologiczne, które stało się przedmiotem rozważań w czwartej części pracy. Autorka opracowania starała się ukazać korzystny wpływ wykorzystania energii geotermalnej na bezpieczeństwo ekologiczne. Przedstawione w pracy propozycje i rozwiązania mogą stanowić inspirację dla państw borykających się z poważnym wyzwaniem dla ekologii, jakie stanowi niska emisja.

Kolejna część pracy poświęcona jest innemu, ważnemu zarówno dla bezpieczeństwa wewnętrznego państwa, jak i bezpieczeństwa międzynarodowego, zagadnieniu wojny hybrydowej i wykorzystaniu w niej działań o charakterze zamachów z użyciem urządzeń wybuchowych. Sfery bezpieczeństwa międzynarodowego

dotyczy również kolejne opracowanie, które, obok przedstawienia międzynarodowych przepisów prawnych dotyczących zwalczania handlu ludźmi, stara się wskazać możliwości doskonalenia obecnie funkcjonujących narzędzi prawnych w celu skuteczniejszego zwalczania tej formy przestępczości. Poprawa bezpieczeństwa międzynarodowego jest związana nie tylko ze stałymi staraniami społeczności międzynarodowej o poprawę istniejących narzędzi prawnych, ale również z działaniami o charakterze wojskowym, takimi jak np. misje pokojowe i stabilizacyjne. W misjach tych od kilku dekad uczestniczą także żołnierze polscy. Autor kolejnej pracy, wykorzystując osobiste doświadczenia uczestnika misji UNIFIL w Libanie, SFOR w Bośni i Hercegowinie oraz Iraqi Freedom w Iraku, stara się skłonić Czytelnika do dyskusji, która sprawiłaby, że społeczeństwo polskie doceni znaczenie udziału polskich sił zbrojnych w tego rodzaju działaniach i ich rolę w zapewnieniu bezpieczeństwa międzynarodowego. Autor ostatniej części pracy na podstawie badań i obserwacji przeprowadzonych w czasie wizyt studyjnych w Indiach prezentuje wstępną analizę wyzwań, przed jakimi staje ten kraj zarówno na szczeblu ogólnokrajowym, jak i stanowym.

Monografia jest owocem współpracy środowiska naukowego oraz osób zajmujących się bezpieczeństwem i zarządzaniem kryzysowym, skupionych wokół odbywającej się od 2011 roku w Łodzi Konferencji Naukowej „Bezpieczeństwo i zarządzanie kryzysowe". Redaktorzy mają nadzieję, że szerokie spektrum problemów podejmowanych w prezentowanej monografii będzie inspiracją zarówno do uważnej lektury prezentowanych treści, jak i zachętą do podjęcia dalszych wyzwań badawczych w obszarze bezpieczeństwa i zarządzania kryzysowego. Jednocześnie liczymy na to, że oddawana do rąk Czytelników publikacja zachęci kolejne osoby do podjęcia współpracy przy następnych tomach serii.

Zofia Wilk-Woś
Roman Stawicki

William J. Buchanan OBE | w.buchanan@napier.ac.uk
The Cyber Academy, Edinburgh Napier University

Andrew Young
The Cyber Academy, Edinburgh Napier University

Richard Macfarlane
The Cyber Academy, Edinburgh Napier University[1]

Technical and Critical Review of Tor Fingerprinting

Introduction

To investigation agencies the access to Internet-based information can provide a rich source of data for the detection and investigation of crime, but they have struggled against the Tor network for over a decade. Its usage has been highlighted over the years, when, in June 2013, Edward Snowden [MacAskill 2013], used it to send information on PRISM to the Washington Post and The Guardian. This has prompted many government agencies around the World to prompt their best researchers to target cracking it, such as recently with the Russian government offering $111,000.

At the core of Tor is its Onion Routing, which uses subscriber computers to route data packets over the Internet, rather than use publically available routers. One thing that must be said is that Tor aims to tunnel data through public networks

[1] Prof William J Buchanan is a Professor in The Cyber Academy, Edinburgh Napier University (e-mail: w.buchanan@napier.ac.uk). Richard Macfarlane is a lecturer in The Cyber Academy. Andrew Young is a researcher in The Cyber Academy.

and keep the transmission of the data packets safe, which is a similar method that Google uses when you search for information (as it uses the HTTPS protocol for the search).

One of the most widely debated questions in today's society is: "To what extent should we be anonymous online?" [Paine et al. 2007, pp. 526–536]. Regardless of personal stance, it is widely agreed that the matter of online anonymity is of utmost importance as we are now living in a world where an entire generation has been born and raised with the Internet at its fingertips [Prensky 2001, pp. 1–6].

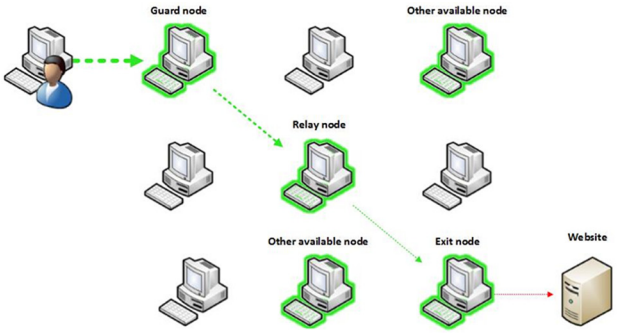
The World Wide Web, however, was not designed with anonymity in mind. In recent times, we have seen a marked rise in the desire to browse and communicate online without any trace being left behind. This demand has led to the development of anonymity networks such as JAP/JonDonym, I2P and specifically, Tor [*Tor Research Home*; Bradbury 2014, pp. 14–17].

Tor is the most secure form of anonymous communication available in current times. Its purpose is to conceal a user's activity on the web from surveillance and traffic analysis. The process it uses to achieve this is known as "onion routing", as shown in Figure 1: data is encrypted upon leaving a device and is then routed through a network of three relays, ran by volunteers, all over the globe. As the data reaches a relay, a layer of encryption is removed from the data and forwarded to the next node in the network, thus providing anonymity to the source of the data and protection against traffic analysis through its encryption.

As we can see in Figure 1, not only does Tor mask a user's IP address but it also encrypts data throughout the process. What this means is that standard traffic analysis can only be conducted on the unencrypted, final relay point (also known as the exit node) in the network.

The purpose of this paper is to investigate the security of the Tor network, evaluate the effect of user profiling through website-fingerprinting attacks and explore improvements which can be made to further secure Tor against them, if any. It will show that while current research in matching users and Web activity to traffic profiles works fairly well in a controlled environment, its performance is often poor in real-life environments.

Figure 1. Simplified view of the Tor network



Source: own work.

Technical review

To truly delve deep into the idea of a website-fingerprinting attack, we must first understand the Tor model and the concepts it is built upon. Throughout this chapter we will explore the world of the deep web, anonymous networking and the core technological components which make it work.

The topic of online privacy has been routinely brought to the public eye over the past few years but very rarely do we see any deep, technical analysis.

A. Anonymity Networks

The purpose of an anonymity network is to provide users with increased privacy while accessing the Internet with various applications providing anonymous communication: Tor, I2P, JAP/JonDonym and Freenet to name a few.

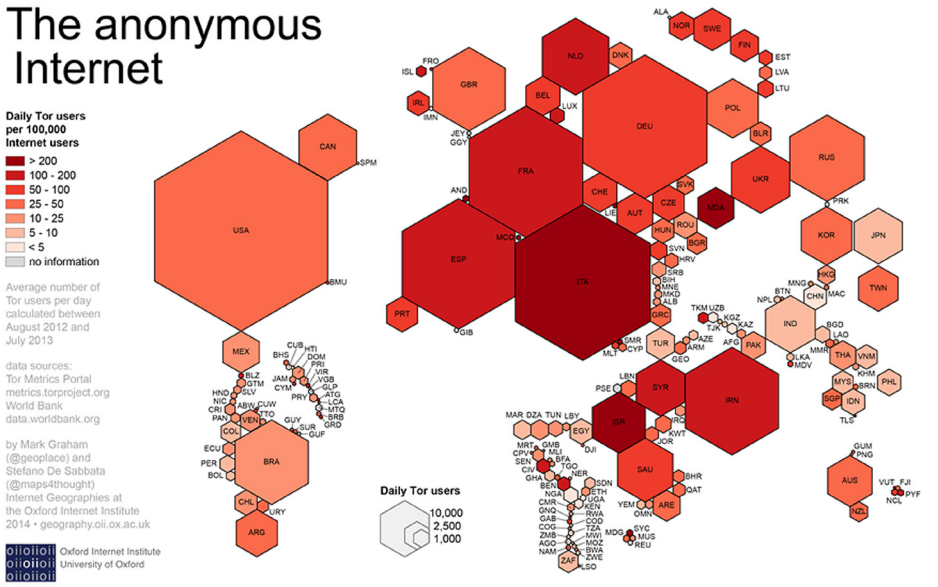
Circumvention of censorship is one of the main uses of anonymity networks with countries such as Belarus, China, Iran and North Korea ranking among the most prolific users of censorship on the web [Morillon, Julliard 2010]. Without the use of these applications, citizens living in these countries would be unable to have the same access to information as those of us in the western-world.

Secure and unidentifiable communication can be critical to those working in politics or journalism, particularly in regions where the state attempts to suppress freedom of the press or any kind of opposition to their government [Cox].

As we become further reliant on the internet and networking technologies, many find that anonymity networks provide protection against various network attacks, traffic analysis or forms of commercial fingerprinting.

An interesting trend shown above is how prevalent Tor usage is in Western countries and specifically, western Europe, where there was public outcry regarding the 2013 security leaks [MacAskill 2013]. We see very high usage of Tor in Saudi Arabia, Israel, Iran and Syria: countries where the current socio-political climate does not enable mass freedom of information but also have ties to the western world due to the presence of journalists, diplomats and military personnel: Tor usage could be from those already in the know or spread via word-of-mouth.

Figure 2. Geographies of Tor – Average number of daily Tor users per day (courtesy of Mark Graham, University of Oxford)



Source: own work.

These applications provide a valuable service to users around the globe, however, they can also be used by malicious people's acts of varying legality.

1. Regions of the Internet

An important first step to understanding the world of internet anonymity is to understand the various terminologies, specifically: the World Wide Web, the Surface Web, the Deep Web and the Dark Web. The World Wide Web is simply defined as the system of interlinked documents which are accessible through

the Internet. The "surface", "deep" and "dark" web are all sub-categories of the World Wide Web.

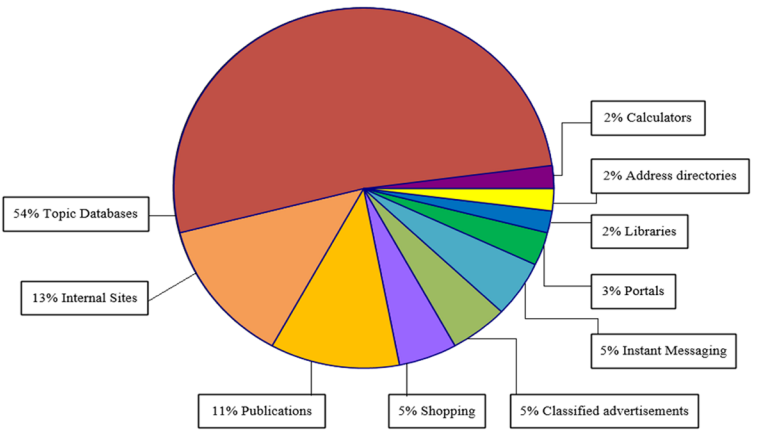
When a standard user of a web-browser such as Chrome, Firefox, Safari or Internet Explorer uses a search engine for their request, they are accessing what is known as the surface web (also known as the; visible web, indexable web, clearnet or surfacenet).

Any content which is not indexed by standard search engines and therefore not accessible through traditional means is categorised as belonging to the deep web. The deep web is effectively the foundation which the rest of the World Wide Web is built on. It is the largest region of the internet and holds the majority of data we use on a day-to-day basis. Much of this is held on servers used by websites, holding data and code used to access pages and documents or on dynamically generated websites which standard search engines do not pick up.

The deep web can be thought of as an all-encompassing region of the internet containing everything from academic journals, private servers and cloud services to online black markets [8] and illegal file-sharing sites. What the deep web is not, is exclusively these services which exist on the fringes of legality.

The main difference between the deep and dark web is that although they are not indexed by standard search engines, the dark web is indexable by Tor. These sites generally take the form of hidden services [Mansfield-Devine 2009] which are only available for use through the Tor browser, which will be covered in greater depth in the following section.

Figure 3. Distribution of deep web sites



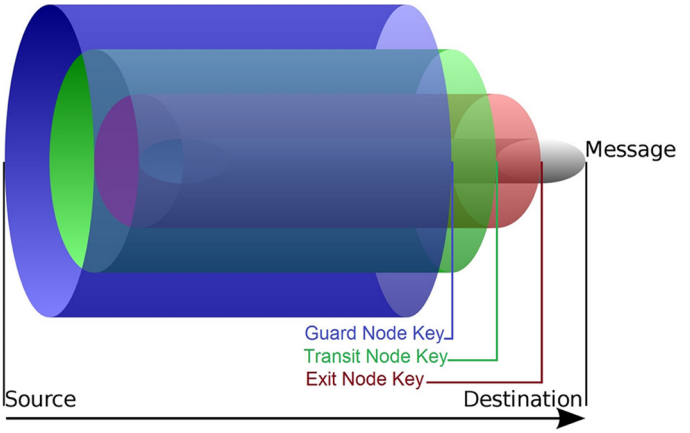
Source: own work.

2. Tor

Tor is an open-source, cross-platform application which provides its users with online anonymity by redirecting and encrypting traffic through a global network of dedicated relays, ran by volunteers. This distributed network is almost completely reliant on volunteers to donate bandwidth to the project by configuring their Tor client to set up their system as a relay. These volunteered systems are the various nodes which make up the Tor network.

The underlying technique behind it's anonymity is a process called onion routing which was initially developed by researchers at the Naval Research Labs in 1998 [Reed, Syverson, Goldschlag 1998, pp. 482–493] as a TCP-based, distributed networking system which capable of anonymizing web-browsing and instant messaging and therefore, providing the US military to communicate securely over the internet without the need to establish infrastructure for a dedicated, private network. The term onion routing derives from the encryption process of the system. At various points along a circuit, a layer of encryption is peeled back before being passed down the line until it reaches its end-point in the network and is readable to the system.

Figure 4. Layers of an onion packet (courtesy of WikiMedia)



Source: own work.

A typical Tor circuit consists of six parties: a directory server, a source, a destination and three relays; guard (also known as entry), transit (also known as relay), and an exit node. The details are:

- The directory server exists to provide the Tor client running on the source with a list of currently available relays.

- Once the source has a list of available nodes to route traffic through, it randomly picks a path consisting of three nodes to route traffic through.
    - Before a packet (referred to as an onion over Tor) is sent, it is encrypted in multiple layers to prevent analysis.
- With the pathway set, data is sent to the guard node which then decrypts the first layer, allowing it to read the source address and destination of the transit node:
    - The transit relay decrypts the second layer and passes the results to the exit node.
    - The exit relay decrypts the third and final layer and passes the results to the destination.
- Data leaving the exit relay and arriving at the destination is unencrypted, however, anyone monitoring this connection will only see a link between the exit node's IP address and the destination's IP address, leaving the source anonymous.
- By default, the Tor client will generate a new, random pathway every ten minutes or when a source changes the destination they wish to access.

The entire process is hidden from the user, who is able to use Tor much like commonly used web-browsers. However, while onion routing itself is an extremely effective way to prevent unwanted persons monitoring traffic, the security of a system is highly dependent on the operator. Tor recently released a statement regarding the use of file-sharing services (specifically; uTorrent, BitTorrent, BitSpirit and libTorrent) on the same system as a user runs a Tor client as researchers from the French Institute for Research in Computer Science and Automation had developed an attack targeting peer-to-peer application users [Manils et al. 2010]. The vulnerability highlighted here was due to torrent traffic being sent over the surface net rather than being diverted through the Tor proxy, an issue which prompted BitTorrent to make use of a Tor network connection by default if detected.

While the likes of I2P and Freenet are decentralised dark nets, Tor relies on its central directory servers to provide information regarding the location of available nodes. While it could mean a network meltdown if these servers go down, it is much easier to secure and monitor a small set of safe servers than to trust this critical routing information to the distributed network.

3. Encryption and path construction

The Tor network transfers data between nodes via TLS connections with a 1024-bit RSA keys [Mathewson]. Inter-relay traffic and the client to guard traffic is done using a single TLS connection which is referred to as a channel in the documentation. By

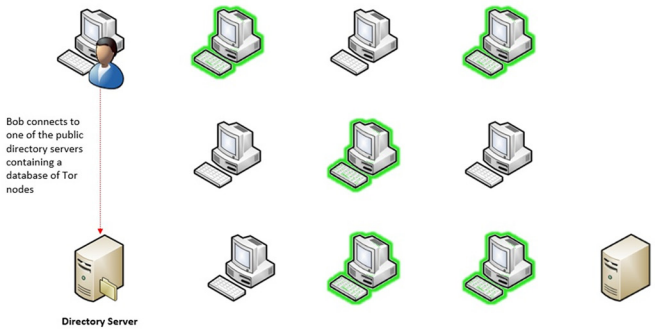
making use of the TLS protocol, Tor conceals the data on the network and prevents an attacker from modifying data on the connection or spoofing the identity of a routing node. Typically, a Tor entry node will be configured to accept these transport-layer frames on ports 9011, 9030 and 9050, also.

Two types of onions are used in the transmission of data: control cells and relay cells. The control cells can be used to bring down, rebuild or create a connection, whereas the relay cells carry the data in a 256-bit AES stream.

- The originator accesses a public key from the directory server to use in cooperation with the guard node.
- Source sends a request to generate a connection and private key with guard node.
- The guard node will then receive an onion from the source in order to choose the next hop destination along with a new public-key to use with the transit node.
- Once the transit-exit node connection is established, the exit node will connect to the end destination specified by the source.
- This final link in the network is not encrypted by Tor but may be secured via HTTPS (as is becoming more common) if the destination supports SSL.

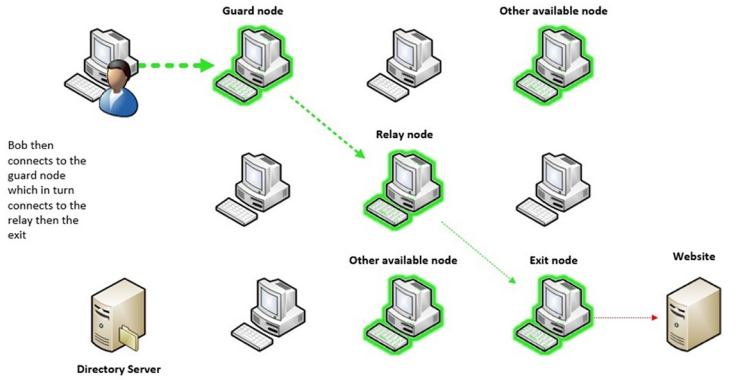
This process is defined as second-generation onion routing [Dingledine 2011]. A major issue in first-generation onion routing was that each node in the network could identify each other node. This vulnerability could be used to threaten an entire system's anonymity should a single node be compromised.

Figure 5. Tor retrieving node listings



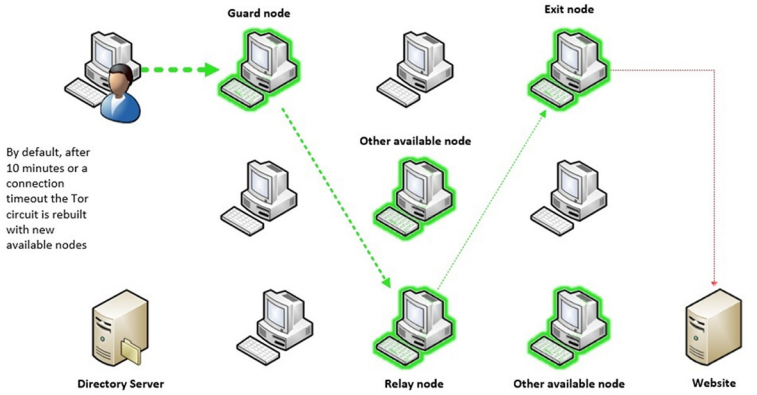
Source: own work.

Figure 6. Tor Circuit Connection



Source: own work.

Figure 7. Tor Circuit Reconfiguration



Source: own work.

Tor traffic uses fixed length cells which flow across the network, and create a circuit, and where each relay node only knows its predecessor and its successor. Each relay node then stores its own symmetric key for the connection and uses this to decrypt cells that are routed through it. For a connection between a client and a server we thus have [Mathewson]:

- **A stream cipher**. This is symmetric key encryption (typically 128-bit AES in counter mode with an IV) for encrypted traffic, and where each relay node has negotiated its key with the server (and which the client will also know).
- **Public-key key encryption**. This uses either 1,024/2,048 bit RSA or Elliptic Curve for identity provision of the relay node.

Elliptic-Curve Diffie-Hellman method for key negotiation. With this only the client and the server will know the keys involved for each of the relay nodes. It uses Curve25519 for the negotiation of the key and which uses the high-speed Elliptic-curve Diffie-Hellman method [Bernstein 2006, pp. 207–228].

- **A hash function.** This is typically SHA-1, and is used to check the integrity of the data cells.

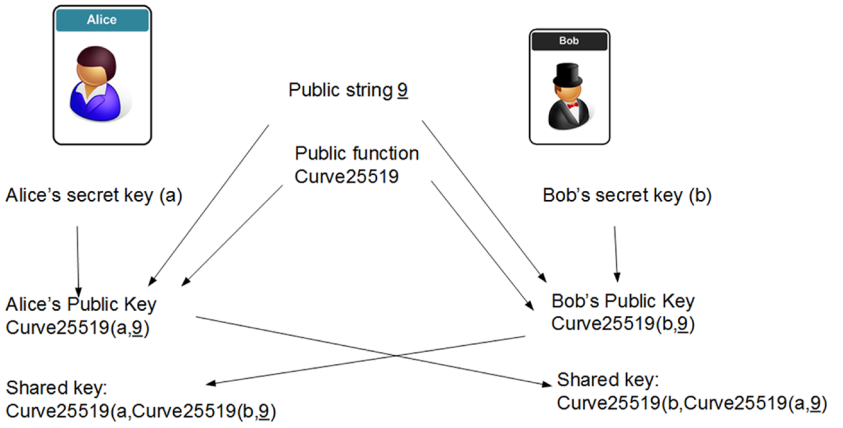
The client or server will initially send a cell and which is encrypted with each of the symmetric keys used in the Tor relay nodes, and encrypted in the sequence where the first relay node has the last encryption key applied (the outer layer of the onion), and the first one used has the key of the last relay node (the inner most layer of the onion). The negotiation of the key that each relay node uses is done on the creation of the circuit with the *ntor* handshake. This uses the Curve25519 method [Bernstein 2006, pp. 207–228] and where the network shares the G and N value.

Along the route, each Tor relay node takes the cell from its predecessor and decrypts with the negotiated symmetric key. It then passes the cell onto its successor. With Curve25519 we generate a 32-byte secret key (256 bits) and a 32-byte public key. A hash of the shared secret is then created as a 32-byte secret key:

(Curve25519(a,Curve25519(b,9))

This is illustrated in Figure 8, and is used to generate a 128-bit AES key.

Figure 8. Key generation for relay nodes



Source: [Bernstein 2006, pp. 207–228].

There are two major vulnerabilities in this process which have been exploited in the past and are still an area of research and development for the Tor Project. The first vulnerability concerns the connection to the directory server wherein if the connection is compromised, an attacker can acquire the address of the guard node to be used in the upcoming Tor chain. While the data being sent to this node will be encrypted, by knowing the IP address an assailant could attempt to bring it down or even be able to correlate the data passing through the node to the source if they have own the guard [Murdoch, Danezis 2005, pp. 183–195]. While this threat has been highlighted in the past, it is highly unlikely to cause any major concern. In the situation where a node is brought down (via DDoS, for example), the Tor circuit will simply reconfigure itself with a new trio of nodes.

The second threat which has caused more drastic damage recently is the chance that of an unsecured guard and exit node. Due to the exit node decrypting the last layer of Tor's encryption, any data sent from it to the destination can be seen in plaintext (as long as the destination does not implement HTTPS). If an adversary has established both a guard and exit node [Cai et al. 2014, pp. 227–238], they could then not only see the contents of the source's packets but also obtain the source's IP address.

4. Tails

While Tor is secure, the types of activities its users engage in are generally the root cause of compromised anonymity. To take secure anonymity a step further, The Tor Project is also developing a live, bare-bones Debian-based distribution which can be booted from a USB or DVD [Loshin 2013; *Tails – Privacy for anyone anywhere*] in the form of Tails: the amnesic, incognito live system. While Tails is generally aimed at typical Tor users, since it is a live operating system, it functions well as a tool for the likes of penetration testers who are seeking an alternative to Kali Linux.

On boot, a system with a mounted version of Tails can choose to run its bespoke operating system instead of the native environment. Tails is delivered as a package which contains various applications a user may wish to use for general computer use, such as; Open Office, Pidgin, Audacity, and GIMP [Loshin 2013]. The requirement for Tails stems from the concept that Tor is only as effective as a user allows it to be. If a system is running various applications such as instant messaging, torrents [Manils 2010], or cloud storage services, the chances that an attacker is able to gain some information greatly increases by using these applications as vulnerabilities and bypassing Tor's security measures. Application leakage is one of the biggest vulnerabilities to onion router users and much of the time it's not the Tor Browser at fault but rather a user not routing their

various data channels through Tor. Alternatively, by using Tails' pre-configured applications only, the security of a system can be vastly improved.

5. Bridges

For most users, the default configuration of the Tor client will suffice, however, it is also capable of routing traffic around firewalls, most notably the "Great Firewall of China" [Winter, Lindskog 2012, pp. 1–2]. In this case, what we see is a two-pronged approach that the Chinese government took to attempt and halt all Tor usage in the country. Firstly, the Tor Project website was censored from Chinese IP addresses, making it very difficult for the news or acquisition of Tor to spread. Secondly, they identified the directory servers used by Tor to inform clients of available nodes which could go on to construct a pathway. The developers of Tor have since implemented a system to bypass the filters imposed on Chinese users: Tor bridges. These bridges act in a similar way to standard relays, however, they are privately and dynamically listed and are only used as a gateway to the greater network.

The deployment of the "Great Firewall of China" has been a clear success for the government. As seen in Figure 2, there are a very small number of daily Tor users in China compared to western nations which share a much higher degree of information freedom. It is clear that when China and Ireland share similar levels of daily Tor users, their firewall has clearly worked in stunting its penetration rates regardless of the development of bridges.

6. Obfsproxy

Used in conjunction with Tor bridges, obfsproxy is a component in the Tor browser bundle which obfuscates the traffic flowing between the client and the desired bridge connection. By doing so, user's in regions such as China, can connect to a Tor bridge and then create a Tor circuit to browse anonymously.

While the Tor network encrypts and proxies traffic, obfsproxy instead transforms network data to appear less suspicious. An area of much development for the Tor Project, obfsproxy supports various plug-ins which allow the user to change the form their traffic will take [*Tor Research Home*] such as transforming onion-routed packets to look like standard HTML, javascript, pdf [Weinberg et al. 2012, pp. 109–120] or even Skype Video packets [Moghaddam, Li 2012, pp. 97–108].

7. Hidden Services

Tor's main aim is to provide users with anonymous access to the surface web, however, it does enable access to areas of the Internet which are generally unreachable.

The region of the dark net visited by Tor user's are home to onion sites: websites who run the Tor Project's hidden services protocol and can be identified by their 16-bit prefix and a URL suffix ".onion" (e.g. 3g2upl4pq6kufc4m.onion). Compared by Tor to "rendezvous points", various Tor users can connect to these hidden service websites, without needing to know any other user's IP address.

A node running a hidden service will first require to advertise its existence across the network before user's will be able to establish a connection to it. To meet this end, the directory server chooses at random certain hidden service relays and constructs routes to them before assigning them as introductory points. In order to act as this first port of call, the node generates a hash table to act as a descriptor containing its public key and a summary of other hidden service node's locations. When a client wishes to access a certain onion site, they will be first routed to the introductory node which holds that sites public key value in its hash table before finally being redirected to their destination.

Simply searching for a list in the surface net brings up a list of various well--known hidden services but many are spread through word of mouth or other offline methods. These hidden services have been marred with controversy in the past [Guitton 2013, pp. 2805–2815; Elsevier Ltd 2013, pp. 1–2].

By the discovery of sites such as The Silk Road, The Marketplace, and illegal pornographic sites. One can imagine that it is the existence of these sites which causes many to argue against further online anonymity. It has been documented in the past [Dinev, Hart, Mullen 2008, pp. 214–233] that some people feel technology such as Tor's hidden services encourage criminal behaviour and provide a hiding spot for drug dealers and sexual offenders, however, these are not new crimes which have been brought on by the advent of the Internet. For every cyber-criminal there are many more scientists, engineers and agents working to maintain the law.

8. Invisible Internet Project: I2P

The Invisible Internet Project is a distributed, overlay network with an emphasis on providing access to its "eepsites" (similar in nature to Tor's onion sites) rather than incognito surface web-browsing, making it a dark web-browser [Zzz, Schimmer 2009, pp. 1–12]. Although I2P is based on onion-routing is actually uses a process it coined "garlic-routing", which is effectively the same in principle. I2P is still under development and currently only the beta release is available (version 0.9.17 as of November 2014) leading to low adoption rates in comparison to its cousin Tor.

Unlike Tor, the I2P network is a de-centralized mesh, meaning that in there are no weak-links which could compromise the security and anonymity of the

system such as the directory servers used in onion routing. It is designed to support dynamic reconfiguration in response to the changing environment. In order to support this distributed system design, the metadata required to route traffic through system is held on a DHT called "netDB". The main benefit of this approach opposed to Tor's centralised directory servers is that the network can be scaled up much easier without placing more pressure on a single node to handle increased traffic as each I2P node carries a copy of the hash table. While this method carries various benefits, it does have its own vulnerabilities such as the "eclipse attack" [Egger et al.] which takes advantage of the Kademlia algorithm used in the construction of the DHT. Earlier versions of I2P had the DHT store data regarding each node involved in the I2P overlay, meaning that if just one node was compromised, every node could be. While the same could be said that in the event of Tor's directory servers being hacked a similar result would occur, it is much easier to secure a small number of nodes that you have full control of than assuming your users will take the same precautions.

With regard to user anonymity, dissimilar to Tor, I2P does not provide asymmetrical anonymity where a user's identity is hidden but not the destination of their traffic. I2P has been built to allow other end-users implementing the I2P service to communicate totally anonymously: it is this symmetrical anonymity which means I2P would not fall prey to the same common attacks that Tor does, such as website-fingerprinting.

In order to implement this symmetrical anonymity, I2P must make use of two unidirectional tunnels: one from source to destination and another from destination to source. In much the same way as Tor, I2P tunnels expire every ten minutes by default in an attempt to lessen the chance that an older tunnel becomes a vulnerability, should a node become compromised.

While the Invisible Internet Project is an interesting take on the world of anonymous networking, it will take some time before it catches up to Tor in terms of security and scale [Moore 2010, pp. 103–117]. Tor simply has more resources at hand and therefore more secure due to the turnaround on updates and larger pool of experts for the peer review process.

9. Freenet

Another popular alternative to Tor is Freenet. Similar to I2P, it is also a distributed, overlay network with an emphasis on peer-to-peer file-sharing. A true darknet, Freenet only gives users the option to browse it's "freesites" which in turn are similar in nature to I2P's eepsites.

A unique provision of Freenet is that users have access to remote, encrypted data storage which is spread out over several nodes which take the form of other connected user's desktops, laptops and mobile devices. Any device which makes use of Freenet will partition a section of their hard-drive or SSD for use as remote storage to the other use, meaning that not only can data be transmitted between nodes securely but the entire system acts as a distributed cloud. The strong encryption used by the network prevents access to the media while also providing "plausible deniability to the nature of the stored data" [Clark 2001, pp. 46–66].

While this could be seen as a fresh alternative to Tor in the event it's encryption has been broken, it is only a matter of time before the encryption used by Freenet is crackable. When this occurs, potentially sensitive data will be stored on a remote user's computer. To mitigate against this threat should it occur, Freenet aims to store files in parts so that no full file is cracked, however, even if partial data recovery could lead to an issue.

10. Telegram

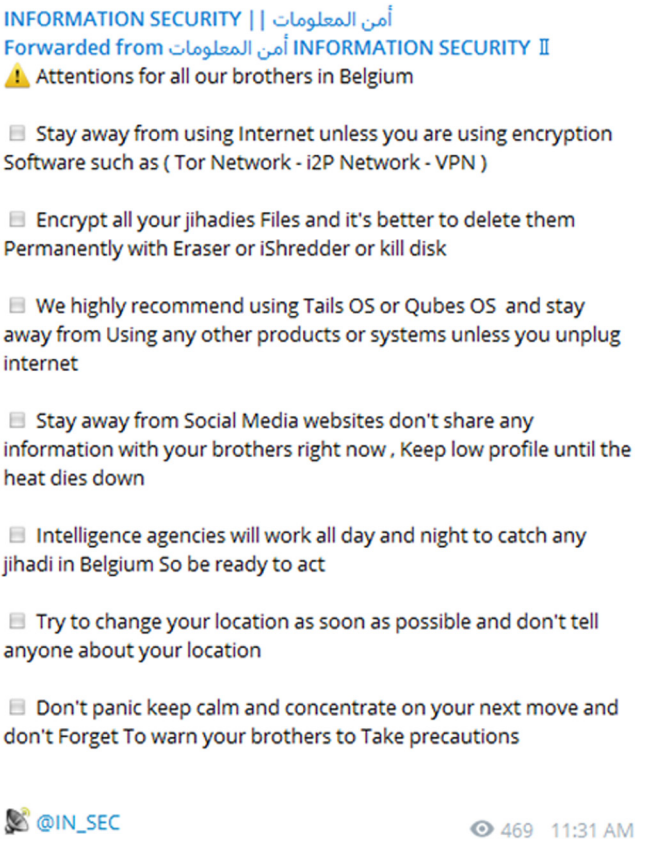
In 2016, the Afaaq Electronic Foundation (AEF), an arm of the Islamic State who are dedicated to "raising security and technical awareness" [*The 3T challenge for digital forensics…*] among jihadists, published their advice on how to avoid law enforcement surveillance. Their message was broadcast on Telegram, with a message of "Stay calm and use strong encryption" (Figure 8).

Telegram provides the usage of heavy encryption, the broadcasting of messages, and in the self-destruction of messages. Within two years of them starting, they had over 100 million active users per month (and over 350,000 new users each day), with over 15 billion messages sent on a daily basis.

Overall Telegram integrates into mobile phone applications using API calls, and converts messages in a binary stream. It then uses cryptography to encrypt the communications before sending it over the network using a range of methods, including for Web communications (HTTP or HTTPS) or network communications (TCP and UDP).

In East Asia, Telegram saw a large number of adoptions for its service since Park Geun-Hye (the South Korean President) announced that users could be prosecuted for insulting or generally rumor-mongering messages, including through private message systems.

Figure 8. Telegram message



Source: own work.

Literature review

Several attacks have been mounted against the Tor network over the years [Manils et al. 2010; Dyer et al. 2012, pp. 332–346; Panchenko, Niessen 2011, p. 103]. Most recently, in the form of website-fingerprinting, peer-to-peer service leakage, and end-to-end correlation attacks. Whilst these active attacks present a clear threat to the security of Tor, another danger comes in the form of human error. No greater example of this is the alleged founder of the Silk Road, Ross Ulbricht (a.k.a Dread Pirate Roberts). What we see here is not a failure in the security of anonymity software but law enforcement executing a system of social engineering to apprehend a suspect.

Although Tor is one of the most secure form of anonymous communication available to the public, there have been several vulnerabilities highlighted over the past few years which have caused major issues. Generally these issues are more prominent at the boundaries of the Tor network, where traffic leaves the security of the relay cluster and ventures back to the surface web where man-in-the-middle, eavesdropping attacks can take place. The most likely circumstance where this sort of threat occurs is if an attacker sets up their own Tor relay exclusively as an exit-node where traffic is finally decrypted.

In the following sub-sections, we will review some of the most serious vulnerabilities of Tor and how the developers have attempted to mitigate their affects.

B. Website-fingerprinting attack

Arguably the largest threat to anonymity on Tor is the website-fingerprinting attack. Whilst the Tor client ensures packets cannot be read using traditional traffic analysis techniques through its onion-encryption process, the website-fingerprinting attack has been proven to be able to accurately ascertain the website a user is accessing.

Before reviewing the various studies regarding this attack, it is important to understand the environment where they take place. Two conditions exist where a website fingerprinting attack can take place: a closed-world and an open-world. The use of open and closed world environments is a common trend in many papers evaluating traffic analysis.

In these scenarios, open world refers to conducting an experiment on the world wide web with no restrictions on the websites a user can visit. A closed world refers to conducting the attack where only a certain set of websites are accessible. Closed-world environments are generally used during the testing phase when conducting the website-fingerprinting attack, allowing developers to review and further expand the program to an acceptable standard. There are several reasons why we make use of both a closed and open world settings, such as to avoid any kind of bias from researchers or simulate the strength of the attack in highly-censored regions.

An important issue to note is the terminology used in most of these papers varies and unless specifically stated when the authors claim that they have developed a system to determine the website accessed while using Tor, it is, in fact, an individual web-page. Due to the nature of the attack and Tor's encryption process, it is extremely to identify entire websites based on the pattern of data and no study has accomplished such, however, it has been possible to identify individual web pages.

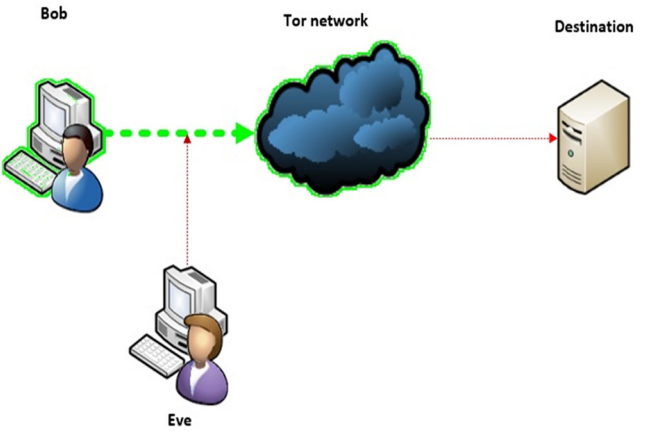
If the example shown in Figure 10 was used as a closed world environment, we assume that the only destinations a victim can visit is limited to Instagram, LinkedIn, Facebook, Tumblr and Twitter. The classifier used to determine a hit from a website-fingerprinting attack could then be tailored to social media sites only, which results in a higher level of accuracy as many of their characteristics will be similar. If the victim is able to access these sites as well as the examples shown to exist in the open world then we will see a drop in accuracy when using the same classifier.

Figure 10. Closed world data set compared to an example of the open world/surface web

Source: own work.

Website-fingerprinting can be performed by a local adversary and can simply be described as a form of complex traffic analysis on encrypted data (Figure 11). The attacker will look for trends in the volume, size, direction of the frequency of bursts of packets to try and obtain information otherwise hidden to them. The attack requires an adversary to monitor traffic flow between a system running the Tor client and the guard node without attempting to break Tor's cryptographic defences. If successful, website-fingerprinting seriously harms the protection and anonymity provided by Tor as it can be carried out by individuals monitoring a local system: instead of dealing with the issue of end-to-end correlation through the distributed relay-network, an attacker can target a user's end system.

Figure 11. Simplified website-fingerprinting attack performed by Eve on Bob



Source: own work.

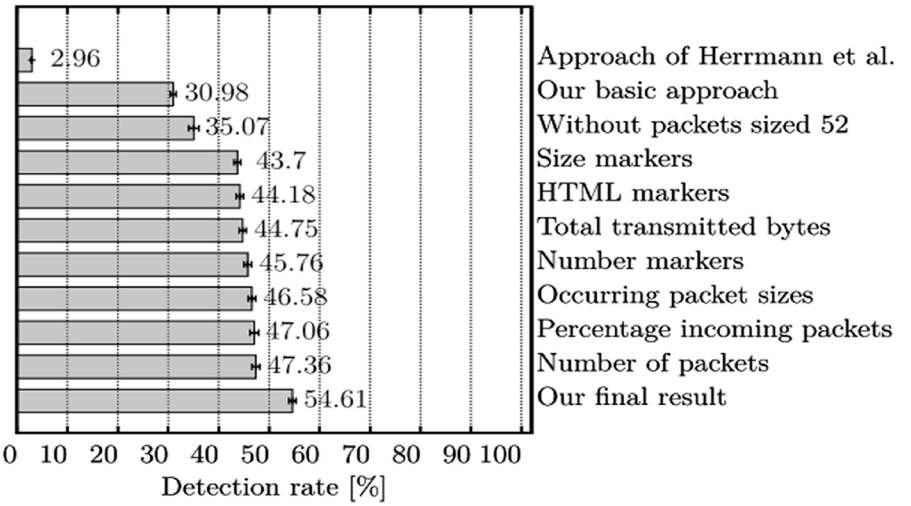
In various papers investigating website-fingerprinting attacks [Wang, Goldberg 2013, pp. 201–212; Cai et al. 2014, pp. 227–238; Dyer et al. 2012, pp. 332–346; Herrmann, Wendolsky, Federrath 2009, pp. 31–41; Panchenko, Niessen 2011, p. 103] closed-world and open world environment were implemented. An open-world scenario is where a user can access any web-page that is online. Typically, we may see malicious Tor nodes who are sniffing traffic flowing through them. This is a passive attack and may be used by ISPs or government authorities to monitor people accessing censored URLs. In this case, attacks may not be interested in other websites visited by the victim and these can be filtered from results which raise a flag. In order to develop this attack, developers require training data which contains both censored and uncensored instances.

The concepts behind the website-fingerprinting attack is relatively simple. Mounting such an attack is not the largest issue facing those conducting it but rather the development of a profiling system to recognise patterns and disregard packets such as TCP handshakes or those related to websites which are not censored or worthy of surveillance. It is important to develop these filters as the capture would otherwise be flooded with useless data, resulting in less accurate profiling, as discussed in the paper by [Panchenko, Niessen 2011, p. 103]. In this situation, the author's disregarded any packets of a size of 52-bytes from their website-fingerprinting software as the SYN and ACK packets skewed results due to their large numbers.

In 2011, Panchenko and Niessen [2011, p. 103] Figure 12, published their paper on website-fingerprinting on the Tor and JAP networks showing that they could

recognise which website a system using Tor was accessing with a 55% true-positive rate on a sample of 775 URLs by classifying a website based on several metrics: volume, timing, and direction of packets. Having conducted their closed-world study with such a large set of web pages, they have shown that their specific attack is much more reliable than those present in other papers, meaning that this study was the largest and most comprehensive to date and has since been used as a basis for research in the papers by [Dyer et al. 2012, pp. 332–346; Cai et al. pp. 227–238], in 2012.

Figure 12. Bar graph showing initial success rate against iterations of website-fingerprinting designed by Panchenko and Niessen in an open-world environment (courtesy of Panchenko, Niessen)



Source: [Panchenko, Niessen 2011, p. 103].

While not reporting the highest levels of accuracy, Panchenko's paper [Panchenko, Niessen 2011, p. 103] is by far the most reliable. Not only have they used the same, large data-set as Herrman, Wendolsky and Federrath [2009, pp. 31–41] but have used a large 4,000 URL data-set taken from Alexa's web statistics service as well as a random 1,000 URLs at their discretion for their open-world experiment. The advantage for using such a large set of web pages is that various types of website can be analysed: it is much harder to identify destinations with dynamic content such as news and media websites than those with static or near-static content such as search engine homepages.

Although more recent papers have reported a much higher success rate when correctly identifying the web page a victim was visiting whilst using the Tor system, significantly smaller sample sizes have been used. Building on this work, Dyer et al offer an analysis of website-fingerprinting attack countermeasures. Although not explicitly reviewing the attack's effect on Tor, we can draw many comparisons as they investigate the use of WPA encryption along with proxy servers relaying HTTP traffic through an encrypted tunnel back to a user as well as the use of Tor alongside other defensive solution.

An unfortunate downside to the work done by Dyer et al. [2012, pp. 332–346], is that they have only conducted their experiment in a closed-world environment meaning that their results are open to bias as the system they were attacking could have been operated by one of the team and their code could be tailored to specifically detect a true-positive result. While this somewhat discredits their findings to a degree, they are the only paper which has looked at conducting a website-fingerprinting attack in relation to such a variety of defensive conditions. Moreover, Dyer et al. [2012, pp. 332–346] claim that at the time of publication: "...in the context of website identification, it is unlikely that bandwidth-efficient, general purpose traffic analysis countermeasures can ever provide the type of security targeted in prior work".

While this may be a strong statement for their research, it is incredibly specific with its wording and is clearly there to reinforce a bias to their paper. By specifying that bandwidth-efficient countermeasures to website-fingerprinting will never work, they disregard options such as traffic morphing and extreme packet flooding [Coull et al. 2007, pp. 35–47] where a Tor circuit floods the network with useless data in order to throw off a traffic analysis attack's classification. However inefficient this may be, under the right circumstances it could provide a level of security high enough to defend against user-profiling. While also stating that they are referring to general purpose analysis this also ignores the fact that many determined assailants could develop a bespoke website-fingerprinting classifier to fit the already known browsing habits of a chosen user.

Following on from the work done by Dyer et al. [2012, pp. 332–346], a further study was carried out the next again year by Cai et al. [2014, pp. 227–238] who reported a 77% success rate when implementing a website-fingerprinting attack. Due to the significantly smaller size of their closed-world sample and no evidence of a study using an open-world environment, the work done by Panchenko and Niessen [2011, p. 103] still appears much stronger in comparison. Despite this, they have tackled the newly implemented defence developed by Tor to pad packets to 512-bytes as standard (which Tor now refer to as cells or onions interchangeably).

From this they have determined that the evaluation of packet sizes for website fingerprinting attacks yields no benefit and have instead focused on the remaining metrics which can be passively eavesdropped: packet timing, flow direction, packet count and packet density.

In 2013 Wang and Goldberg [2013, pp. 201–212] published their paper regarding a modified website-fingerprinting attack which was based on the source code published by Cai et al. [2014, pp. 227–238] the previous year. This study was the first time that Tor control onions were removed from the web page classification algorithm and has shown that more accurate results are achievable when they are disregarded as they claim to have a true-positive rate of 91% in their 100-page closed-world environment. The control packets were noted to be of 52-bytes only, rather than the standard 512-bytes for transmission packets.

In order to further evaluate the effectiveness of their attack, Wang and Goldberg [2013, pp. 201–212] looked at some of the more difficult sites to identify using current classifiers in an attempt as to why these had such low detection rates. News and media websites were proven to be the hardest to classify, especially those with localised content for users in other countries (e.g. BBC News displays different headlines to Brits than to Americans). The difficulty occurs due to the fact that the website-fingerprinting classifier has been developed to identify a static web page whereas news and media websites frequently update their content. They suggest that website-fingerprinting attacks could be mitigated against if a website is designed with more dynamic content on display. With this in mind, we can come to the conclusion that the less frequently a website updates its content, the more vulnerable it is to identification through website-fingerprinting fingerprinting.

The surface web, the deep web, and the dark web are inherently different entities. In none of the papers investigating website-fingerprinting attacks do they state that the web-pages which are being identified are exclusive to the dark web (such as .onion pages) and thus only reachable through the Tor network. This shows that although this attack is a threat to the majority of Tor users, those who are using it as a means to access sites such as The Silk Road or various hidden services are not affected.

Along with analyzing timings within accesses to Web sites, researchers have identified patterns of activity within the usage of standard Web page components, such as with JavaScript. In [Mulazzani et al.] the researchers identify UserAgent string modifications in order to detect the JavaScript engine fingerprinting, and which is used in the Tor browser bundle as it uses a uniform UserAgent string.

Table 1. Comparison of results from previous website-fingerprinting attack papers

	Wang and Goldberg	Cai et al.	Dyer et al.	Panchenko and Niessen
Publication date	2013	2013	2012	2011
Success rate	91%	77.5%	82%	55%
Closed world data set	100	100	2	775
Open world data set	None	None	None	5,000

Source: own work.

C. Peer-to-peer leakage

Outwith the threat of calculated attacks on the Tor network, many of the failures to the network's security comes from the end users themselves. Although the dangers of peer-to-peer information leakage are not entirely derived from human interaction, they can be mitigated against through the secure configuration of an operating system and the adoption of browsing habits uncommon to many users. Peer-to-peer leakage has been proven to provide an assailant with a victim's IP address and can be used as a precursor to performing a website-fingerprinting attack, should the requirement arise.

The peer-to-peer information leakage vulnerability was brought to light for the Tor community in 2014 through the paper authored by Manils et al. [2010]. The paper itself stemmed from reports from Chinese users that the Great Firewall of China had begun shutting down Tor bridge relays, further increasing the level of censorship in the region. The attack itself does not directly target Tor but instead aims to deanonymize users by attacking peer-to-peer file-sharing applications in order to acquire information which would otherwise by hidden through the use of Tor. While the paper looks specifically at BitTorrent, it does touch on those who use other similar applications such as uTorrent or libTorrent.

For peer-to-peer connections to work, IP addresses must be exchanged in order to create a connection. When a user wishes to share a file they establish a seed which is indexed and searchable through various torrent search sites. The BitTorrent application makes use of directory servers known as trackers which pair up a user's request with known seeds, leading to a P2P connection. What this means for those wishing to hide their identity is that of a tracker is compromised, the attacker has a list of all the IP addresses who are downloading a specific file; this could have severe consequences in situations where the data being downloaded

is deemed as contraband. A natural step to prevent this would be to use Tor to proxy a system's address [Brian, McDermott, Weins 2011, pp. 135–136].

By default, BitTorrent will operate on the surface web but can be configured to make use of the Tor network to mask the details of whatever files are being transferred and who is involved, however, the tracker will always require a user's IP address in order to match it to a seeder. BitTorrent implements a system wherein it selects a random, ephemeral port (typically in the range of numbers 49,152 to 65,535) designated for each file transmission and sends this information to the tracker. In doing so, the tracker now has an IP address and a port which has a high likelihood of being unused by any other peer establishing a connection to the specific seeder.

With this in mind, if a tracker has been compromised or a malicious exit node exists between a Tor user and a seeder, an attacker can identify a user's IP address and although the TCP connection is anonymised through Tor, can scan the systems open ports and correlate this to determine what and where you are transferring.

While they exist as two very different threats to Tor, if an individual is subject to a successful P2P leakage attack it can be just the stepping stone to the destruction of anonymity. All an adversary needs to perform a website-fingerprinting attack is the IP address of a user.

D. User profiling

One of the challenges for investigators is to pin-point the traffic that relates to given users. In [Gonzalez, Soriente, Laoutaris 2016, pp. 373–379] the research team tracked within HTTPS and found that match network traffic analysis to user interests, demographic types, and other information. They did this, though, by investigating the destination address, which is not possible within a Tor network. For sites which have a strong signature for its network activity, it was possible to match users to their interests. Along with this users can often be matched from the Internet behaviors, and which match to the activity footprint. In [Wang 2013 et al.] users were successfully matched using the behaviors of 16,000 real and Sybil users from Renren [Yang et al. 2014].

E. Current work

Juarez et al. [2014, pp. 263–274], in 2014, carried out a critical approach on Website Fingerprinting (WF), and outlined that user's browsing habits and differences in location and version of Tor Browser Bundle, were normally omitted from attack models.

Recently Wang [Wang, Goldberg 2016, pp. 21–36] outlines that while researchers have managed to fingerprint Tor traffic under lab conditions, there are significant differences with a realistic environment. In particular, they highlight that it may not be possible for an attacker to continually update their training set, and also where trained sequences in the lab will relate to single Web pages and trained on the first packet sent, and where noise is often added to the captured traffic due to network traffic from other pages. They present several new methods which are able to address the problems they highlight, and where packets can be collected in the wild.

He et al. [He et al. 2014, pp. 112–117] also outline the problems related to the overlapping of Web accesses, and propose a method where the attacker delays HTTP requests that originated from users, in order to isolate their requests. For this they manage to identify access to the Alexa Top 100 top websites with a greater success than previous work.

Within [Kwon et al. 2015, pp. 287–302], the authors defined weaknesses in the creation of hidden services that can reveal their operation. This, they propose, is because these circuits – the paths established within the Tor network – behave differently to general circuits. For this they define two attacks that can reveal a hidden service client., with a true positive rate of 98% true positive rate.

The POSTER [Mitseva et al. 2016] attack uses a two-phase fingerprinting approach to discover hidden services. They outline that most of the methods used to the present have depended on attacking different version of Tor, and that in their system, the attacker on the link between the client and the first anonymization node, and can attack the connection to any hidden service. To overcome the placement of the attacker on the first connection between the client and the first node, the PIVOT system [Yang Xue, Vasserman 2016, pp. 765–773] can be placed anywhere in the route and fingerprints using traffic volume and timing information. They work has been assessed against real human behavior than against scripted traffic activity.

Within TORBEN [Arp, Yamaguchi, Rieck 2015, pp. 597–602], an attack involves web pages being manipulated to load content from untrusted origins identifies the request-response traffic flows. They sourced 60,000 web pages, and detected over 91% of the access pages, with no false positives.

While most of the work has focused on attacking the Tor network, some researchers have focused on reducing the opportunities for attack. In [Juarez et al. 2016, pp. 27–46], the researchers uses an adaptive Padding method that protects against website fingerprinting, and reduces the chances of detection from 91% to 20%, while adding in zero latency, and less than 60% bandwidth overhead.

While analyzing timings is still a focus for many detection systems, [Jahani, Jalili 2016, pp. 43–51] uses a Fast Fourier Transform to convert timing information into the frequency domain, and where the feature extraction overhead can be reduced by a factor of 400. Within a closed-world simulation, they gain a minimum success rate of 95%.

Conclusions

The challenge of the Tor network provides a major challenge for investigators, and while researchers have managed to compromise it, it has managed to heal itself. The usage of fingerprinting techniques thus seems to be one of the few methods left which can effectively discover hidden services, but these have perhaps not scaled well from the lab environment to a real-life investigation. Within [Wang, Goldberg 2016, pp. 21–36] the authors defined the main problems within fingerprinting as:

- Conducted in a closed world. This world often does not match a realistic investigation scenario.
- Lack of replicability. Data capture often matches to the methods used in the fingerprinting process.
- Non-realistic browsing behaviour. Users often load page after page in a sequential manner.
- Non-realistic page load parsing. The methods often know where page loads start and end.
- No background traffic. Often there is no background traffic which significantly improves detection rates.

References

Arp D., Yamaguchi F., Rieck K. (2015), *Torben*, Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security – ASIA CCS '15, pp. 597–602.

Bernstein D.J. (2006), *Curve25519: New Diffie-Hellman Speed Records*, Springer, Berlin, Heidelberg, pp. 207–228.

Bradbury D. (2014), *Unveiling the dark web*, "Netw. Secur.", No. 4, pp. 14–17.

Brian D., McDermott P., Weins J. (2011), *WikiLeaks is a wake-up call for openness*, "Government Information Quarterly", Vol. 28, No. 2. pp. 135–136.

Cai X., Nithyanand R., Wang T., Johnson R., Goldberg I. (2014), *A Systematic Approach to Developing and Evaluating Website Fingerprinting Defenses*, Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur. – CCS '14, pp. 227–238.

Clarke I., Sandberg O., Wiley B., Hong T. (2001), *Freenet: A distributed anonymous information storage and retrieval system* [in:] H. Federrath (ed.), *Designing Privacy Enhancing Technologies*, Berkeley, CA, USA, pp. 46–66.

Coull S.E., Wright C.V., Monrose F., Collins M.P., Reiter M.K. and others (2007), *Playing Devil's Advocate: Inferring Sensitive Information from Anonymized Network Traces*, "Ndss", Vol. 7, pp. 35–47.

Cox J., *Countries that Use Tor Most Are Either Highly Repressive or Highly Liberal – Motherboard* [online], https://motherboard.vice.com/en_us/article/8q8xga/countries-that-use-tor-most-are-either-highly-repressive-or-highly-liberal, access: 13.07.2017.

Dinev T., Hart P., Mullen M.R. (2008), *Internet privacy concerns and beliefs about government surveillance – An empirical investigation*, "J. Strateg. Inf. Syst.", Vol. 17, No. 3, pp. 214–233.

Dingledine R. (2011), *Measuring the safety of the Tor network*.

Dyer K.P., Coull S.E., Ristenpart T., Shrimpton T. (2012), *Peek-a-boo, I still see you: Why efficient traffic analysis countermeasures fail*, Proceedings – IEEE Symposium on Security and Privacy, pp. 332–346.

Egger C., Schlumberger J., Kruegel C., Vigna G., *Practical Attacks Against The I2P Network* [online], https://sites.cs.ucsb.edu/~chris/research/doc/raid13_i2p.pdf.

Elsevier Ltd (2013), *Silk Road online drug market taken down*, "Netw. Secur.", Vol. 2013, No. 10, pp. 1–2.

Gonzalez R., Soriente C., Laoutaris N. (2016), *User Profiling in the Time of HTTPS*, Proceedings of the 2016 ACM on Internet Measurement Conference – IMC '16, pp. 373–379.

Guitton C. (2013), *A review of the available content on Tor hidden services: The case against further development*, "Comput. Human Behav.", Vol. 29, No. 6, pp. 2805–2815.

He G., Yang M., Gu X., Luo J., Ma Y. (2014), *A novel active website fingerprinting attack against Tor anonymous system*, Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2014, pp.112–117.

Herrmann D., Wendolsky R., Federrath H. (2009), *Website fingerprinting: attacking popular privacy enhancing technologies with the multinomial naïve-bayes classifier*, Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 31–41.

Jahani H., Jalili S. (2016), *A novel passive website fingerprinting attack on tor using fast fourier transform*, "Comput. Commun.", Vol. 96, pp. 43–51.

Juarez M., Afroz S., Acar G., Diaz C., Greenstadt R. (2014), *A Critical Evaluation of Website Fingerprinting Attacks*, Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur. – CCS '14, pp. 263–274.

Juarez M., Imani M., Perry M., Diaz C., Wright M. (2016), *Toward an Efficient Website Fingerprinting Defense*, Springer International Publishing, pp. 27–46

Kwon A., Alsabah M., Lazar D., Dacier M., Devadas S. (2015), *Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services*, "USENIX Secur.", pp. 287–302.

Loshin P. (2013), *Practical Anonymity*, Syngress.

MacAskill E. (2013), *Edward Snowden: how the spy story of the age leaked out*, "The Guardian".

Manils P., Abdelberri C., Le Blond S., Kaafar M.A., Castelluccia C., Legout A., Dabbous W. (2010), *Compromising Tor Anonymity Exploiting P2P Information Leakage*, Arxiv Prepr. arXiv10041461.

Mathewson N., *Tor's protocol specifications* [online], https://gitweb.torproject.org/torspec.git/tree/tor-spec.txt, access: 26.07.2017.

Mitseva A., Panchenko A., Lanze F., Henze M., Wehrle K., Engel T. (2016), *POSTER: Fingerprinting Tor Hidden Services* [online], https://www.comsys.rwth-aachen.de/fileadmin/papers/2016/2016-mitseva-ccs-fingerprinting.pdf.

Moghaddam H.M., Li B. (2012), *SkypeMorph: Protocol obfuscation for Tor bridges*, Proc. 2012 ACM Conf. Comput. Commun. Secur., pp. 97–108.

Moore T. (2010), *The economics of cybersecurity: Principles and policy options*, "Int. J. Crit. Infrastruct. Prot.", Vol. 3, No. 3–4, pp. 103–117.

Morillon L., Julliard J. (2010), *Enemies of the Internet: Web 2.0 versus Control 2.0*, Reporters Without Borders [online], http//www. rsf. org/ennemis. html.

Mulazzani M., Reschl P., Huber M., Leithner M., Schrittwieser S., Weippl E., *Fast and Reliable Browser Identification with JavaScript Engine Fingerprinting* [online], http://www.ieee-security.org/TC/W2SP/2013/papers/s2p1.pdf.

Murdoch S.J., Danezis G. (2005), *Low-cost traffic analysis of Tor*, Proceedings – IEEE Symposium on Security and Privacy, pp. 183–195.

Paine C, Reips U.D., Stieger S., Joinson A., Buchanan T. (2007), *Internet users' perceptions of 'privacy concerns' and 'privacy actions*, "International Journal of Human-Computer Studies", Vol. 65, No. 6, pp. 526–536.

Panchenko A., Niessen L. (2011), *Website fingerprinting in onion routing based anonymization networks*, Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, pp. 103–114.

Prensky M. (2001), *Digital Natives, Digital Immigrants Part 1*, "Horiz.", Vol. 9, pp. 1–6.

Tor Research Home [online], https://research.torproject.org/index.html, access: 8.01.2017.

Reed M.G., Syverson P.F., Goldschlag D.M. (1998), *Anonymous connections and onion routing*, "IEEE J. Sel. Areas Commun.", Vol. 16, No. 4, pp. 482–493.

Tails – Privacy for anyone anywhere [online], https://tails.boum.org/, access: 08.01.2017.

The 3T challenge for digital forensics: Tails, Telegram and Tor | William Buchanan | Pulse | LinkedIn [online], https://www.linkedin.com/pulse/3t-challenge-digital-forensics-tails-telegram-tor-william-buchanan, access: 8.01.2017.

Wang T., Goldberg I. (2013), *Improved website fingerprinting on Tor*, Proc. 12th ACM Work. Work. Priv. Electron. Soc. – WPES '13, pp. 201–212.

Wang G., Konolige T., Zheng H., Zhao B.Y., Wilson C., Wang X. (2013), *You Are How You Click: Clickstream Analysis for Sybil Detection*, "Usenix Security", 14, pp. 241–256.

Wang T., Goldberg I. (2016), *On Realistically Attacking Tor with Website Fingerprinting*, "Proc. Priv. Enhancing Technol.", Vol. 2016, No. 4, pp. 21–36.

Weinberg Z., Wang J., Yegneswaran V., Briesemeister L., Cheung S., Wang F., Boneh D. (2012), *StegoTorus: A Camouflage Proxy for the Tor Anonymity System*, Proc. 2012 ACM Conf. Comput. Commun. Secur., pp. 109–120.

Winter P., Lindskog S. (2012), *How China Is Blocking Tor*, Free Open Commun. Internet, [online], https://arxiv.org/pdf/1204.0447.pdf., pp. 1–2.

Yang Z., Wilson C., Wang X., Gao T., Zhao B.Y., Dai Y. (2014), *Uncovering Social Network Sybils in the Wild*, "ACM Transactions on Knowledge Discovery from Data (TKDD) – Casin special issue", Vol. 8, Iss. 1.

Yang Xue, Vasserman E.Y. (2016), *Simple and compact flow fingerprinting robust to transit through low-latency anonymous networks*, 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 765–773.

Zzz, Schimmer L. (2009), *Peer Profiling and Selection in the I2P Anonymous Network 1 I2P Overview*, Present. PET-CON 2009, pp. 1–12.

Roman Stawicki | rstawicki@spoleczna.pl
Społeczna Akademia Nauk

Jerzy Bieńkowski | jbienkowski@spoleczna.pl
Społeczna Akademia Nauk

Bezpieczeństwo w szkole – na podstawie opinii maturzystów

Wstęp

Zapewnienie bezpieczeństwa i poczucia bezpieczeństwa stanowi istotne zadanie dla każdego człowieka, grupy społecznej czy państwa. W tym kontekście środowisko szkolne, w którym wzrasta przyszłe pokolenie, stanowi wspólną sferę odpowiedzialności, lecz przede wszystkim wyzwanie stojące przed rodzicami oraz nauczycielami. Prawidłowy przebieg procesu kształcenia i rozwoju wymaga współdziałania różnych podmiotów w celu wyeliminowania wszelakich zagrożeń występujących w przestrzeniach prywatnych i publicznych, w tym w szkole. Dorośli powinni nauczyć dzieci i młodzież przewidywania zagrożeń, unikania ich, a w sytuacjach kryzysowych – radzenia sobie z trudnościami. Bezpieczeństwo jest zobiektywizowanym stanem braku zagrożeń, a poczucie bezpieczeństwa stanowi subiektywny, niekiedy wręcz emocjonalny aspekt życia każdego człowieka. Dlatego analizując zjawiska kryminogenne, należy wyróżnić dwa kierunki działania. Pierwszy wykorzystuje „obiektywne" dane statystyczne gromadzone przez służby, straże, inspekcje itp. Natomiast drugi kierunek obejmuje badania opinii społecznej nad postrzeganiem tych zjawisk i lękiem przed nimi na podstawie często subiektywnych przesłanek.

Z kolei analizując pojęcie zagrożeń bezpieczeństwa, zwłaszcza na poziomie lokalnym, można je określić jako różnego rodzaju czynniki, które m.in. godzą w wartości, warunki życia i zdrowia, mienie czy środowisko człowieka. W dotyczącej

bezpieczeństwa literaturze przedmiotu występuje wiele klasyfikacji zagrożeń, w zależności od przyjętego kryterium, skali zagrożeń, ich źródeł oraz skutków. Warto też podkreślić, iż zapewnienie bezpieczeństwa i poczucia bezpieczeństwa w szkole to nie tylko wyzwania dla szkoły, a także innych podmiotów odpowiedzialnych za te obszary życia młodego pokolenia. Stąd też realizacja projektu badawczego pt. *Bezpieczeństwo w szkole – wspólnym dobrem*, którego wyniki i wnioski zaprezentowano w niniejszym artykule.

Celem głównym przeprowadzonych badań było zdiagnozowanie bezpieczeństwa i poczucia bezpieczeństwa maturzystów w środowisku szkolnym, jak również określenie najważniejszych czynników mogących obniżyć poziom ewentualnych zagrożeń. Realizacji tak sformułowanego celu służyły następujące problemy badawcze:

1. Jakie funkcje pełni szkoła jako środowisko edukacyjne oraz społeczno-wychowawcze?
2. Jakie poczucie bezpieczeństwa w Polsce, w miejscu zamieszkania i w diagnozowanych szkołach mają uczniowie?
3. Co i dlaczego stanowi szczególne zagrożenie dla maturzystów w szkole?
4. Jakie są deklaracje uczniów związane ze współuczestnictwem w kształtowaniu bezpieczeństwa?

Podstawową metodą wykorzystywaną w przygotowaniu artykułu był sondaż diagnostyczny. Ponadto zastosowano analizę ilościowo-jakościową dokumentacji oraz literatury naukowej, a także wnioskowanie. Przedmiotem badań objęto funkcjonowanie wybranych szkół ogólnokształcących i techników, których uczniowie brali udział w kursach przygotowujących do egzaminów dojrzałości z przedmiotu matematyka, realizowanych przez Społeczną Akademię Nauk.

Funkcje szkoły jako środowiska edukacyjnego oraz społeczno-wychowawczego

Szkoła jako wartość społeczna oraz podstawowa instytucja kształcenia, zajmowała i nadal zajmuje przeważającą pozycję w wychowaniu oraz zapewnieniu odpowiednich warunków rozwoju uczniom, spośród instytucji i placówek prowadzących bezpośrednią działalność oświatowo-wychowawczą. Termin „szkoła" wywodzi się z języka greckiego od „skhole", który oznaczał „wczasy", „spokój", „czas poświęcony nauce", zaś czasownik „szkolić" miał dość uszczuplone znaczenie, gdyż wiązał się tylko z czynnościami, takimi jak: nauczanie, prowadzenie wykładów, poświęcanie się

czemuś [Kupisiewicz 2005, s. 177]. Prawdopodobnie w czasach nowożytnych szkoła stała się przeciwieństwem tego, za co uważali ją starożytni Grecy: charakteryzowała się napiętą atmosferą, pracą, strofowaniem oraz świadomymi i systematycznymi procesami, których celem było wpojenie człowiekowi określonych ideologii i doktryn, zwłaszcza politycznych i społecznych [http://www.sjp.pwn.pl]. Definicję leksykalną szkoły zawierają różnego rodzaju słowniki i opracowania encyklopedyczne. Zgodnie z wyjaśnieniem zawartym w *Encyklopedii Popularnej,* szkoła oznacza:

1) instytucję oświatowo-wychowawczą;
2) budynek szkolny;
3) system instytucji;
4) wykształcenie osiągnięte w takiej instytucji;
5) kierunek w nauce, filozofii, literaturze itp., którego przedstawicieli łączą wspólne podstawowe poglądy i metody pracy twórczej (np. polska szkoła matematyczna, krakowska szkoła historyczna, szkoła kantowska w filozofii [Encyklopedia Popularna, t. 1, s. 58].

Współcześnie oświata odgrywa bardzo ważną rolę i stanowi wspólne dobro całego społeczeństwa. Fundamenty edukacji stanowią zasady zawarte w Konstytucji RP z 1997 r. [Dz. U. z 1997 r. nr 78 poz. 483], a także zalecenia wynikające z Powszechnej Deklaracji Praw Człowieka, Międzynarodowego Paktu Praw Obywatelskich i Politycznych oraz Międzynarodowej Konwencji o Prawach Dziecka. Szkoła jest jednostką oświatowo-wychowawczą, która zajmuje się kształceniem oraz wychowaniem młodych ludzi zgodnie z podstawą programową oraz Ustawą z dnia 7 września 1991 r. o systemie oświaty [Dz. U. z 2018 r. poz. 1457, 1560]. Wychowanie kształtuje i rozwija u dzieci poczucie odpowiedzialności, miłości do ojczyzny oraz poszanowania dla polskiego dziedzictwa kulturowego. Dlatego też szkoła odpowiedzialna jest za przygotowanie do pełnienia obowiązków rodzinnych i obywatelskich. Szkoła jako instytucja oświatowo-wychowawcza oznacza zatem miejsce, w którym dzieci i młodzież przebywają razem przez określony czas i poddawane są regularnym procesom nauczania, według opracowanego wcześniej planu, który został sporządzony w ramach funkcjonującego systemu oświaty.

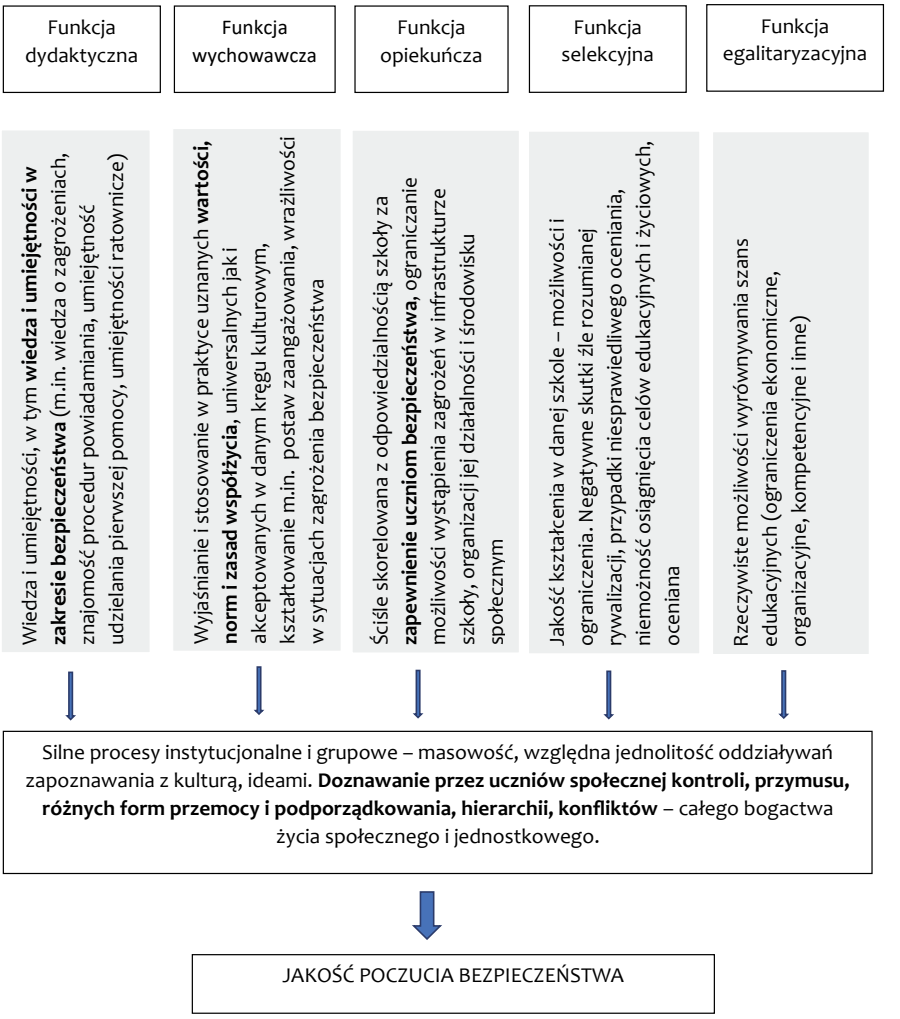
Obecnie szkoła wspólnie z rodziną i grupą rówieśniczą w największym stopniu oddziałuje na zachowanie młodzieży. Zasadniczą jej funkcją jest przygotowanie człowieka do dorosłości poprzez wdrażanie do czterech rodzajów norm społecznych: niezależności, dokonań, uniwersalności i szczególności [Karkowska 2010, s. 182]. Są to normy umożliwiające każdemu człowiekowi funkcjonowanie w społeczeństwie. Jednocześnie szkoła może przyczyniać się do zagrożenia uniformizacją, konserwacją zastanych warunków społecznych [Aronson, Wilson,

Akert 2006, ss. 216, 223, 227]. Wydaje się, że żadna z teorii próbujących opisać rolę szkoły w społeczeństwie nie jest w stanie ukazać złożoności jej oddziaływania na jednostkę, jak również wpływu bliższego i dalszego otoczenia społecznego na człowieka. Od szkoły oczekuje się, że będzie skupiona na uczniu, że jej działalność będzie związana ze społeczeństwem, a ona sama jednocześnie będzie stanowić określony system społeczny (uczniowie, nauczyciele, kierownictwo, pracownicy administracyjni), poddawany silnemu oddziaływaniu rodziców, systemu politycznego, różnych ideologii, mediów, gospodarki i innych ośrodków społecznego wpływu.

Wśród funkcji szkoły najbardziej oczywista i wywołująca prawdopodobnie najmniej kontrowersji jest funkcja dydaktyczna, polegająca na systematycznym uprzystępnianiu wiedzy spełniającej kryteria naukowe, społeczne i dydaktyczne, rozwijaniu zdolności i kształtowaniu zainteresowań uczniów. Szkoła, wyjaśniając i stosując w praktyce uznane wartości, normy i zasady współżycia, uniwersalne i akceptowane w danym kręgu kulturowym, spełnia też funkcję wychowawczą. Pokładane są w niej nadzieje na ukształtowanie osobowości uczniów opartych na systemie wartości, a przejawiających się w postawach, odgrywaniu ról i zachowaniach. W szkole zachodzą silne procesy instytucjonalne i grupowe, to w nich, poprzez masowość, względną jednolitość oddziaływań uczniowie zapoznawani są z kulturą, ideami, ale doznają również społecznej kontroli, przymusu, różnych form przemocy i podporządkowania, hierarchii, konfliktów – całego bogactwa życia społecznego i jednostkowego [Aronson, Wilson, Akert 2006, ss. 179, 245].

Z kolei funkcja opiekuńcza realizowana jest poprzez zapewnienie dzieciom opieki, zwłaszcza w czasie pozalekcyjnym i pozaszkolnym (świetlica i organizowane tam formy aktywności, koła zainteresowań), co nie oznacza, iż funkcja ta nie bywa sprawowana w czasie lekcji razem z funkcją wychowawczą (np. interwencja w razie pojawienia się konfliktu). Ponadto funkcja opiekuńcza szkoły jest ściśle skorelowana z odpowiedzialnością szkoły za zapewnienie uczniom bezpieczeństwa (rys. 1).

Rysunek 1. Bezpieczeństwo na tle funkcji szkoły



Źródło: opracowanie własne.

Dyrekcja szkoły, wychowawcy, właściwie wszyscy pracownicy szkoły powinni, stosownie do kompetencji i uwarunkowań sytuacyjnych, podejmować działania dla bezpieczeństwa środowiska szkolnego. Współdziałanie wymienionych osób jest konieczne chociażby z tego względu, że przyczynami wypadków w szkołach są najczęściej [https://bezpiecznaszkola.men.gov.pl/...]:

1. braki w wiedzy o stanie i potrzebach szkoły w dziedzinie bezpieczeństwa i higieny, nieprzeprowadzane przeglądy i pomiary, lekceważone zagrożenia i nieznajomość przepisów;
2. niewystarczające finansowanie infrastruktury szkoły ograniczającej zagrożenia;
3. zaniedbania w organizacji czasu spędzanego przez ucznia w szkole: (podczas lekcji i przerw);
4. zagęszczenie, nadmiar bodźców, hałas;
5. nieadekwatny do potrzeb system norm wewnątrzszkolnych;
6. niekonsekwentne reagowanie, czy wręcz bagatelizowanie niepożądanych zachowań osób z środowiska szkolnego, nieudolne rozwiązywanie konfliktów;
7. pojawianie się nowych zagrożeń, jak zagrożenia w cyberprzestrzeni czy terroryzm.

Wypełnianie funkcji opiekuńczej wiąże się nierozłącznie z potrzebą podejmowania odpowiednich działań profilaktycznych w środowisku fizycznym szkoły i terenie bezpośrednio do niej przyległym (monitorowanie, nadzór) oraz wśród uczestników procesu dydaktyczno-wychowawczego. Wymieniane w literaturze socjologicznej, pedagogicznej i psychologicznej [Karkowska 2010, s. 187; Kowalik 2011, s. 274; Konarzewski 2005, s. 84] inne funkcje szkoły, to jest selekcyjna i egalitaryzacyjna, tylko z pozoru mają znacznie mniejsze oddziaływanie na powstawanie zagrożeń w środowisku szkolnym. Ocenianie, nieodłączny element procesu kształcenia, jest bardzo silnym przejawem funkcji selekcyjnej szkoły. Możliwości sprawowania przez szkołę funkcji egalitaryzacyjnej (wyrównywania szans edukacyjnych) są ograniczone dostępnymi środkami finansowymi, rozwiązaniami organizacyjnymi, kompetencjami nauczycieli, motywacją i innymi czynnikami. W rezultacie, uzyskiwane oceny i rzeczywiste możliwości wyrównywania szans przyczyniają się do kształtowania jakości poczucia bezpieczeństwa.

Z jednej strony, szkoła wyposażając uczniów w wiedzę i umiejętności pozwalające poznawać i rozumieć rzeczywistość przyrodniczą, społeczną, poznawać innych ludzi i samego siebie – sprzyja realizacji celów życiowych [Niemczyński 1988, s. 224], wpływa tym samym na poczucie bezpieczeństwa z perspektywy całego życia. Z drugiej strony, szkoła jest odzwierciedleniem społeczeństwa, w którym funkcjonuje. Zachodzą w niej silne procesy instytucjonalne i grupowe, uczniowie doznają społecznej kontroli, przymusu, różnych form przemocy i podporządkowania, hierarchii i konfliktów. W pełni uzasadnione zatem jest ujmowanie poczucia bezpieczeństwa również w bardzo krótkiej perspektywie czasowej, nawet sytuacyjnej. Szkoła, zwłaszcza poprzez nauczycieli i rówieśników, sprawia iż wszystkie sukcesy i porażki, temperament, emocje, osobowość ucznia i innych

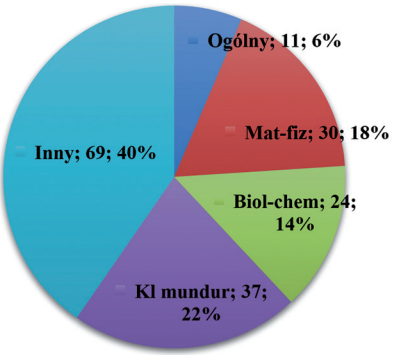
uczestników procesów dydaktyczno-wychowawczych, mają publiczny wydźwięk [Ratajek 2007, ss. 23–28], a poczucie bezpieczeństwa jest następstwem relatywnej deprywacji, osobistych i przez to subiektywnych porównań własnych osiągnięć z sukcesami i porażkami innych.

Charakterystyka respondentów – wybrane cechy socjodemograficzne

Badania zostały przeprowadzone w okresie od początku kwietnia do końca maja 2018 r. wśród uczniów klas maturalnych, którzy brali udział w kursach przygotowujących do egzaminów dojrzałości z przedmiotu matematyka, realizowanych przez Społeczną Akademię Nauk. Ogółem w badaniach uczestniczyło, na zasadzie dobrowolności, 203 respondentów. Po wstępnej weryfikacji zgromadzonego materiału badawczego do dalszych analiz wykorzystano 171 kwestionariuszy ankiety, pozostałe odrzucono ze względu na braki odpowiedzi na niektóre pytania. Dobór badanych miał charakter losowy, a wielkość próby badawczej i jej struktura nie były reprezentatywne w stosunku do populacji osób przystępujących do egzaminów maturalnych. Do matury w 2018 roku przystąpiło około 272 600 zdających, którzy ukończyli liceum ogólnokształcące lub technikum w roku szkolnym 2017/2018 [https://cke.gov.pl/images/_KOMUNIKATY...]. Wśród ankietowanych było: 114 kobiet (66,6%) i 57 mężczyzn (33,3%).

Badaniami objęto młodzież uczęszczającą do dwóch rodzajów szkół średnich tj. liceum ogólnokształcące (73%) oraz technikum (23% uczestniczących w badaniach). Kolejną zmienną opisującą respondentów był profil kształcenia (wykres 1). Przedstawiciele klas mundurowych stanowili 22% ankietowanych. Natomiast profil matematyczno-fizyczny reprezentowało 18% osób. Kolejne profile według wielkości procentowego udziału to biologiczno-chemiczny (14%) i ogólny (6%). Jednak dominującą kategorię, bo aż 40%, stanowili uczniowie, którzy zaznaczyli odpowiedź „inny profil kształcenia".

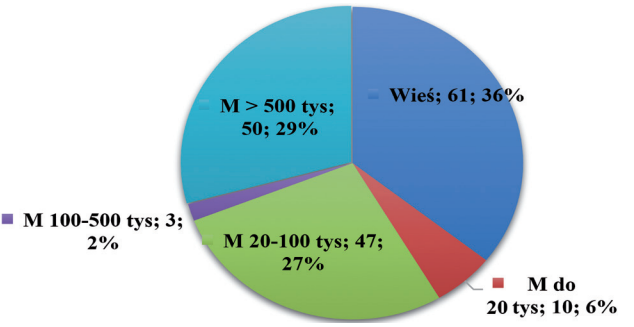
Wykres 1. Profil kształcenia respondentów



Źródło: opracowanie własne.

Grupę najliczniejszą (36%) ze względu na miejsce zamieszkania badanych stanowili mieszkańcy wsi (wykres 2). Drugą co do wielkości częścią próby badawczej (29%) były osoby, które zdeklarowały jako miejsce zamieszkania miasto powyżej 500 tys. Nieco mniej (27%) przebywało w mieście od 20 do 100 tys. Tylko 10 ankietowanych (6%) zamieszkiwało w miastach do 20 tysięcy.

Wykres 2. Miejsce zamieszkania badanych



Źródło: opracowanie własne.

Jak już wspomniano, próba badawcza nie była reprezentatywna, ponadto byli to wyłącznie uczestnicy kursu przygotowującego do egzaminu dojrzałości z matematyki. Pomimo tych ograniczeń opinie badanych mogą stanowić podstawę do poznania określonych trendów, a co za tym idzie, wyciągania wniosków i uogólnień formułowanych z myślą o podniesieniu jakości szeroko rozumianej edukacji dla bezpieczeństwa.

Ocena poczucia bezpieczeństwa w Polsce, w miejscu zamieszkania i w diagnozowanych szkołach

Definicje leksykalne utożsamiają bezpieczeństwo z brakiem zagrożenia i poczuciem pewności. W słowniku języka polskiego „bezpieczeństwo" zdefiniowano jako stan psychiczny lub prawny, w którym jednostka ma poczucie pewności, oparcie w drugiej osobie, lub w sprawnie działającym systemie prawnym, przeciwieństwo zagrożenia [*Uniwersalny Słownik Języka Polskiego* 2007, s. 50]. Z kolei poczucie bezpieczeństwa ma charakter indywidualnego odczuwania najrozmaitszych stanów, odnosi się nie tylko do bezpieczeństwa, ale także poczucia istnienia, stanu zadowolenia czy też szczęścia. Najogólniej poczucie bezpieczeństwa można określić jako fizyczne i psychiczne odczuwanie spokoju i pewności. Do subiektywnych czynników i jednocześnie elementów poczucia bezpieczeństwa najczęściej zalicza się: poczucie stabilności sytuacji życiowej i możliwość jej przewidzenia, poczucie poinformowania (rezultat edukacji i dostęp do bieżących informacji), odczuwanie sensu własnego życia, posiadanie planów i perspektyw życiowych, bliskie relacje i silne więzi z bliskimi i określonymi kręgami społecznymi, odczuwanie istnienia norm prawnych i moralnych dotyczących sprawiedliwości, ładu i porządku (nie tylko publicznego), umiejętność identyfikowania zagrożeń [Dziurzyński, Sawicki 2009, ss. 8–9; Marciniak 2009, ss. 60–61; Szweda 2016, s. 137, 158].

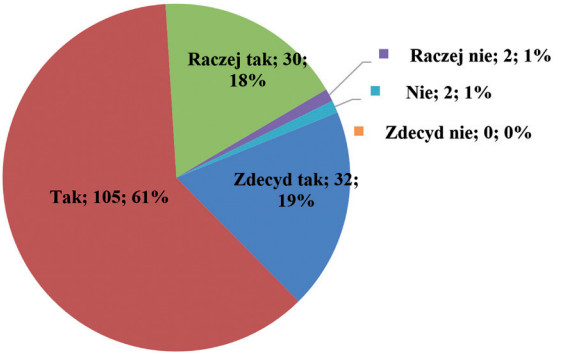
Jedną z istotnych cech poczucia bezpieczeństwa jest jego zmienność. Po pierwsze, związane jest ono ściśle z poszczególnymi etapami życia, dokładniej – przechodzeniem z jednych do kolejnych. Dodatkowo jest ono skorelowane z postępowaniem instynktownym, redukującym niepewność poprzez działania orientacyjno-nawykowe, ograniczanie możliwości bycia zaskoczonym. Poczucie bezpieczeństwa, jego poziom i ewolucja w przebiegu całego życia, jest uwarunkowane wzrastającymi wraz z rozwojem jednostkowym możliwościami działań percepcyjnych, wspieranymi procesami poznawania i rozumienia otoczenia przyrodniczego, rzeczywistości społecznej, poznawania innych ludzi oraz siebie samego. Procesy poznawcze są też wzbogacane postępującym doświadczeniem życiowym. W efekcie dążenia człowieka do kształtowania bezpiecznych interakcji ze środowiskiem przyrodniczym i szeroko rozumianym społecznym powodują, że jest on skuteczny w realizacji swoich celów życiowych [Niemczyński 1988, s. 224]. Po drugie, dynamika poziomu poczucia bezpieczeństwa wynika z uwarunkowań sytuacyjnych i jej perspektywa czasowa może być krótka, poczucie bezpieczeństwa zależy od stanu emocjonalnego, stresu, strachu, ale też od temperamentu i osobowości. Poczucie bezpieczeństwa zatem jest następstwem relatywnej deprywacji, subiektywnych porównań własnych sytuacji z sytuacjami innych.

Zarówno w perspektywie całożyciowej, jak i ograniczonej wydarzeniami krótkotrwałymi, przejściowymi, nawet epizodami sytuacyjnymi, niezwykle ważne jest dysponowanie adekwatną wiedzą. Wiedza o różnych rodzajach i aspektach bezpieczeństwa jest czynnikiem zmiany jakości poczucia bezpieczeństwa. Przy czym, co należy zaznaczyć, wzrost poziomu i zakresu posiadanej wiedzy nie tylko pozytywnie oddziałuje na jakość poczucia bezpieczeństwa, w pewnych warunkach może przyczynić się do zwiększonego odczuwania zagrożeń. Jednak co do zasady, poczucie bezpieczeństwa zależy nie tyle od stwierdzania określonych zdarzeń i procesów, co od ich trafnej oceny, a w dokonywaniu oceny (porównań) konieczne jest odwoływanie się do posiadanej wiedzy jako formy reprezentacji rzeczywistości przyrodniczej i społecznej, w której występują różne zagrożenia. Poprzez to, że wiedza ta jest spersonalizowana, przyjmuje postać względnie uporządkowanej i wzajemnie powiązanej struktury [Nęcka, Orzechowski, Szymura 2008, s. 137].

Instytucjonalne i osobiste kształtowanie poczucia bezpieczeństwa jest związane z przetwarzaniem wiadomości w umyśle ludzi. Odnosi się do cyklu poznawczego oraz tworzenia poznawczej rzeczywistości. Sposób postrzegania rzeczywistości społecznej oraz innych ludzi jest zależny od zdobytych doświadczeń, potrzeb i aktualnych celów życiowych, od właściwości umysłu, stanów emocjonalnych odczuwalnych w danym miejscu i czasie. Zatem poczucie bezpieczeństwa ma charakter emocjonalny oraz intelektualny, który można kształtować poprzez zastosowanie mechanizmów działania społeczności [Sulowski, Brzeziński 2009, s. 59].

Poczucie bezpieczeństwa maturzystów zbadano na trzech poziomach: krajowym, lokalnym i w miejscu nauki. Wyniki uzyskane podczas badania prezentują kolejne wykresy (3–5). W przypadku poczucia bezpieczeństwa w skali Polski dominowała odpowiedź „Tak" – 61%. Kolejna grupa respondentów wybrała odpowiedź „Zdecydowanie tak" – 19%. Odpowiedź „Raczej tak" zaznaczyło 18% ankietowanych. Zatem suma pozytywnych ocen dotyczących indywidualnego odczuwania stanu bezpieczeństwa w Polsce ukształtowała się na poziomie aż 98%. Warto podkreślić, iż nikt z badanych nie wybrał odpowiedzi „Zdecydowanie nie".

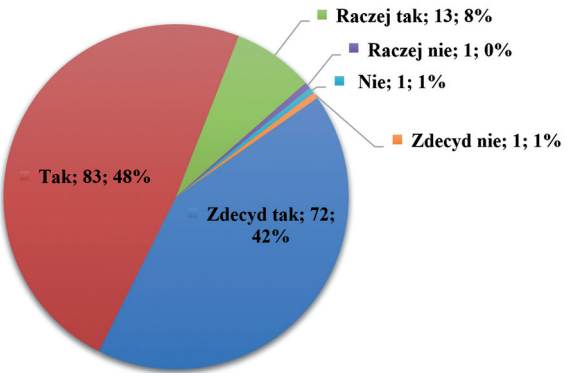
Wykres 3. Czy czujesz się bezpiecznie w Polsce?



Źródło: opracowanie własne.

Natomiast analizując procentowy rozkład odpowiedzi dotyczących poczucia bezpieczeństwa w miejscu zamieszkania, należy zauważyć znaczący wzrost udziału odpowiedzi „Zdecydowanie tak" w porównaniu do pytania nr 1 – „Czy czujesz się bezpiecznie w Polsce?". W odniesieniu do miejsca zamieszkania respondenci ponaddwukrotnie częściej deklarowali zdecydowane poczucie bezpieczeństwa. Przy czym skumulowane pozytywne odpowiedzi były takie same jak w odniesieniu do poziomu ogólnokrajowego. Tylko 1% badanych zaznaczył kategorię „Zdecydowanie nie". Najprawdopodobniej było to spowodowane własnymi doświadczeniami lub opiniami członków społeczności lokalnej.

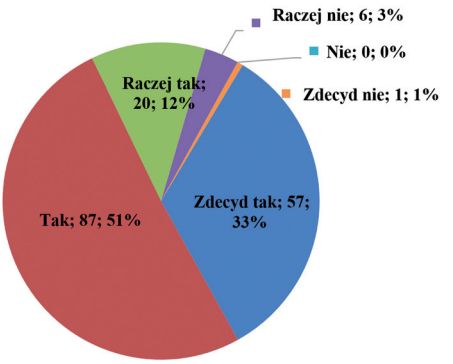
Wykres 4. Poczucie bezpieczeństwa w miejscu zamieszkania



Źródło: opracowanie własne.

Nieco inne wyniki uzyskano w odniesieniu do środowiska szkolnego. W nim aż 96% ankietowanych czuło się bezpiecznie. Jednak udział kategorii odpowiedzi „Zdecydowanie tak" (33%) był o 9% niższy niż w przypadku poczucia bezpieczeństwa w środowisku lokalnym. Nastąpił też wzrost liczby respondentów wybierających odpowiedź „Raczej nie" do 3%, porównując z pytaniem nr 1.

Wykres 5. Poczucie bezpieczeństwa w szkole



Źródło: opracowanie własne.

Analizę zależności pomiędzy poczuciem bezpieczeństwa na różnych poziomach a płcią badanych prezentuje tabela nr 1. Dane w niej zawarte wskazują na to, iż płeć nie miała większego wpływu na poczucie bezpieczeństwa maturzystów, zwłaszcza w szkole.

Tabela 1. Poczucie bezpieczeństwa w Polsce, w miejscu zamieszkania i w szkole w zależności od płci respondentów

Poczucie bezpieczeństwa N=171		*Kobiety*		*Mężczyźni*		*Łącznie badani*	
		n	*%*	*n*	*%*	*n*	*%*
W Polsce	Skumulowane odpowiedzi „zdecydowanie tak", „tak", „raczej tak"	111	z licz. 66,47 z płci 97,37	56	z licz. 33,53 z płci 98,24	167	98
	Skumulowane odpowiedzi „raczej nie", „nie", „zdecydowanie nie"	3	z licz. 75,00 z płci 2,63	1	z licz. 25,00 z płci 1,76	4	2

Poczucie bezpieczeństwa N=171		Kobiety		Mężczyźni		Łącznie badani	
		n	%	n	%	n	%
W miejscu zamieszkania	Skumulowane odpowiedzi „zdecydowanie tak", „tak", „raczej tak"	111	z licz. 66,07 z płci 97,37	57	z licz. 33,93 z płci 100	168	98
	Skumulowane odpowiedzi „raczej nie", „nie", „zdecydowanie nie"	3	z licz. 100,00 z płci 2,63	0	z licz. 0,00 z płci 0,00	3	2
W szkole	Skumulowane odpowiedzi „zdecydowanie tak", „tak", „raczej tak"	112	z licz. 66,67 98,24	56	z licz. 33,33 98,24	168	98
	Skumulowane odpowiedzi „raczej nie", „nie", „zdecydowanie nie"	2	z licz. 66,67 z płci 1,76	1	z licz. 33,33 z płci 1,76	3	2

Źródło: opracowanie własne.

W kontekście poczucia bezpieczeństwa na poziomie szkoły interesujące może być poznanie czynników, które zdaniem badanych mają największe znaczenie dla ich bezpieczeństwa w środowisku szkolnym. Wydaje się, że najlepszym sposobem ukazania istotnych determinantów będzie ich zestawienie z uwzględnieniem procentowego udziału zarówno pod względem liczby odpowiedzi, jak i liczby badanych/przypadków. Zaakcentowania wymaga fakt, że ankietowani mogli wskazać maksymalnie trzy czynniki. Z tego powodu dane dotyczące badanych/przypadków nie sumują się do 100%.

Tabela 2. Liczbowy i procentowy udział czynników o najważniejszym znaczeniu dla bezpieczeństwa w szkole (badani mogli wskazać maksymalnie trzy czynniki)

Czynniki znaczące dla bezpieczeństwa w szkole N=171	n	Procent względem liczby odpowiedzi	Procent względem liczby badanych/ przypadków
Dobre relacje między nauczycielami i uczniami	112	25,06	65,50
System kontroli wchodzących do szkoły	45	10,07	26,31
Monitoring wewnątrz szkoły	62	13,87	36,26
Monitoring wokół szkoły	30	6,71	17,54
Dobre relacje pomiędzy uczniami	103	23,04	60,23

Czynniki znaczące dla bezpieczeństwa w szkole N=171	n	Procent względem liczby odpowiedzi	Procent względem liczby badanych/ przypadków
Dyscyplinująca działalność nauczycieli	28	6,26	16,37
Działalność samorządów uczniowskich	18	4,03	10,53
Profilaktyka	49	10,96	28,65
Razem	447	100,00	261,39

Źródło: opracowanie własne.

Najwięcej osób (112) wybrało czynnik „Dobre relacje między nauczycielami i uczniami". Stanowili oni 65,5% w stosunku do ogólnej liczby badanych oraz 25,06% względem liczby odpowiedzi. Tuż za tą relacją znalazły się dobre więzi pomiędzy samymi uczniami (103 wskazania), czyli 60,23% wobec liczby badanych/ /przypadków, a także 23,04% względem liczby odpowiedzi. Zdecydowanie mniejsze znaczenie przypisywano następującym czynnikom: monitoringowi wokół szkoły, dyscyplinującej działalności nauczycieli i działalności samorządów uczniowskich.

Zagrożenia bezpieczeństwa w szkole w opiniach maturzystów

W ostatnich latach termin „zagrożenie" rozwinął się na szeroką skalę, co wiąże się z jego występowaniem w literaturze, poświęconej edukacji, psychologii, ekonomii czy medycynie. Geneza tego terminu nie jest dokładnie sprecyzowana. Często nauczyciele posługują się nim do opisu dzieci, które są narażone na niebezpieczeństwo wypadnięcia z systemu edukacyjnego, czy do opisu młodzieży, która nie opanowała umiejętności potrzebnych do radzenia sobie po ukończeniu nauczania bądź do scharakteryzowania dzieci, których poziom nauczania prawdopodobnie jest zbyt słaby, aby kontynuować nauczanie w szkole. Inni zaś uważają, że termin „zagrożenie" nierozerwalnie łączy się z „ryzykiem", które opisuje zespół mechanizmów przyczynowo-skutkowych. Narażają one dzieci i młodzież na negatywne sytuacje w przyszłości. Jeśli dziecko pali papierosy, istnieje prawdopodobieństwo, że po pewnym czasie będzie spożywało alkohol. Jeżeli pije alkohol, prawdopodobnie zażyje miękkie narkotyki. Młodzież, która odważyła się wziąć miękkie narkotyki, w przyszłości może być zagrożona uzależnieniem od narkotyków. Dlatego też uważa się, że zachowanie czy postawa dzisiaj jest wyznacznikiem tego, co będzie jutro [McWhirter, McWhirter, McWhirter 2001, ss. 34–36].

Z uwagi na to, że szkoła we współczesnych czasach nie jest miejscem bezpiecznym, trzeba starać się eliminować ewentualne zagrożenia. Wiąże się to z tym, że niezbędne jest w pierwszej kolejności rozpoznanie źródła ich pochodzenia. Przy czym należy pamiętać, że niebezpieczeństwa grożące dzieciom w szkole mogą pochodzić z różnych źródeł. Zagrożenia generalnie możemy podzielić na: wewnętrzne, zewnętrzne i pośrednie:

1) zagrożenia wewnętrzne charakteryzują się tym, iż stwarzają je sami uczniowie, są to jedne z najczęściej ignorowanych zagrożeń występujących w instytucji szkolnej: ucieczki z lekcji, bójki, wymuszenia pieniędzy;

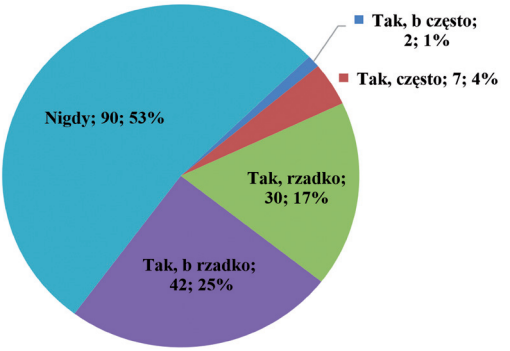
2) zagrożenia zewnętrzne: ataki terrorystyczne, podłożenia bomby, zagrożenia przyrody. Do tych zagrożeń potrzebne jest zabezpieczenie placówki przed osobami postronnymi oraz odpowiednie przeszkolenie w zakresie zagrożeń wywołanych siłami przyrody;

3) zagrożenia pośrednie – mamy z nimi do czynienia, kiedy biorą w nich udział osoby z zewnątrz oraz uczniowie: narkotyki, broń, działalność gangów [Kawula, Konieczny 2005, ss. 57–58].

Stąd niezwykle ważne są wszelkie działania o charakterze zapobiegawczym i profilaktycznym. W tym kontekście opracowany w Ministerstwie Edukacji Narodowej dokument *Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów* jest zbiorem wartościowych informacji i zaleceń w zakresie działalności profilaktycznej w związku z ryzykiem pojawienia się różnorakich zagrożeń w szkole [https://bezpiecznaszkola.men.gov.pl…]. Autorzy uwzględnili też zagrożenia wewnętrzne środowiska szkolnego, do których zaliczyli zachowania agresywne, kradzieże i wymuszenia, środki psychoaktywne, przypadki prostytucji, rozpowszechnianie pornografii, niepokojące zachowania seksualne, niebezpieczne i szkodliwe korzystanie z cyberprzestrzeni.

Z tych względów jednym z celów badawczych było rozpoznanie ilościowe i jakościowe zagrożeń występujących w środowisku szkolnym. Odczuwanie zagrożenia w szkole, na podstawie uzyskanych wyników badań, zobrazowano na wykresie 6.

Wykres 6. Przypadki poczucia zagrożenia w szkole w czasie edukacji respondentów



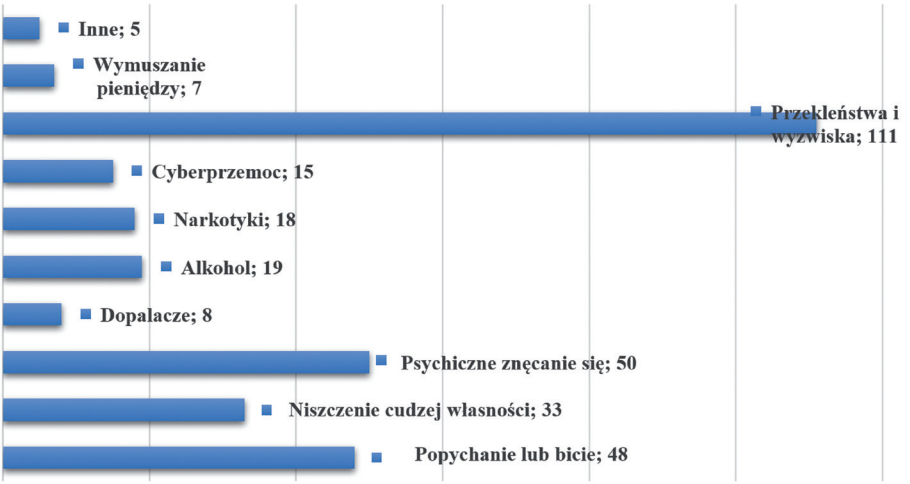
Źródło: opracowanie własne.

Aż 53% uczniów podaje, że nigdy nie odczuwało zagrożenia w szkole (różnice z uwzględnieniem procentowego udziału odpowiedzi ze względu na płeć badanych są niewielkie – kobiety około 52%, mężczyźni około 54%), zaledwie 1% twierdzi, że bardzo często je odczuwało, a 4% często. Zastanawiające mogą być różnice w poczuciu bezpieczeństwa w szkole (wykres 5) i odczuwaniu zagrożenia w niej (wykres 6). Przyczyn rozbieżności w ocenach najprawdopodobniej należy upatrywać w tym, iż przypadki poczucia zagrożenia mogły mieć związek z osobistym doświadczaniem zagrożeń, a w mniejszym stopniu ich zaobserwowaniem.

Zachowania młodzieży ostatniego roku nauki w szkole średniej, skonfrontowane z etapem rozwoju psychospołecznego (m.in. subiektywna postawa wobec wartości, indywidualna waloryzacja społecznych sposobów dochodzenia do uznanych za wartościowe celów – wykształcenie, zawód, pozycja społeczna, coraz bardziej wyrazista koncepcja własnej tożsamości i relacji z innymi), u części młodzieży są manifestowane w sposób oceniany jako zagrażający poczuciu bezpieczeństwa ich najbliższego otoczenia społecznego – rówieśników. Przekleństwa i wyzwiska, psychiczne znęcanie się oraz popychanie lub bicie i niszczenie cudzej własności (wykres 7), to najczęściej wymieniane przez badanych zachowania odbierane jako zagrożenia. Można je uznać za przejawy różnych form agresji w kontaktach społecznych [Matusewicz 2006, s. 312, 313; Obuchowska 2009, ss. 388–390]. Przyczyny tego typu zachowań agresywnych są złożone i mogą być uwarunkowane m.in. ograniczeniem powodzenia w osiąganiu zamierzonych celów, posiadania rzeczy czy chęcią zwrócenia na siebie uwagi. Środowisko szkolne, zwłaszcza jego warstwa instytucjonalna (role, normy, zakazy), znacząco ogranicza, a przynajmniej kierunkuje aktywność uczniów, ponadto skutki rozwarstwienia społeczeństwa,

bezradność i apatia, brutalizacja oddziałują na społeczność szkolną dewaluacją, a nawet głoszeniem pogardy dla społecznie ważnych zasad.

Wykres 7. Kontakt z zagrożeniami na terenie szkoły (przypadki, które wystąpiły w ostatnim czasie)



Źródło: opracowanie własne.

Tabela 3. Liczbowy i procentowy udział zagrożeń spotkanych w szkole (badani mogli wskazać wszystkie 10 odpowiedzi)

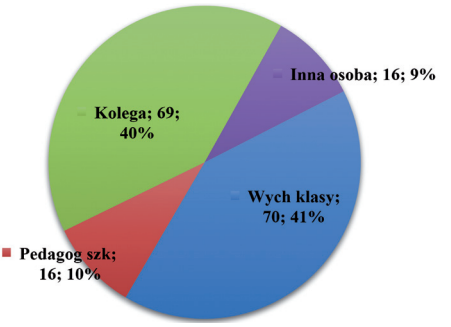
Zagrożenia z którymi respondenci spotkali się w szkole zagrożeniach N=171	n	Procent odpowiedzi	Procent przypadków
Popychanie lub bicie	48	15,29	28,07
Niszczenie cudzej własności	33	10,51	19,30
Psychiczne znęcanie się	50	15,92	29,24
Dopalacze	8	2,55	4,68
Alkohol	19	6,05	11,11
Narkotyki	18	5,73	10,53
Cyberprzemoc	15	4,78	8,77
Przekleństwa i wyzwiska	111	35,35	64,91
Wymuszanie pieniędzy	7	2,23	4,09
Inne	5	1,59	2,92
Razem	314	100,00	183,62

Źródło: opracowanie własne.

Nie tylko przekleństwa i wyzwiska (35,35% odpowiedzi), ale psychiczne znęcanie się (15,92% odpowiedzi), popychanie lub bicie (15,29% odpowiedzi) i cyberprzemoc (4,78% odpowiedzi), mają bezpośredni związek z jakością komunikacji wzajemnej i poczuciem bezpieczeństwa w szkole [Strumska-Cylwik 2011, ss. 54–55]. Uczniowie rzadko pozwalają sobie na bunt wobec nauczycieli i ich wymagań związanych z programem kształcenia, lecz jak ukazują wyniki badań, w stosunku do rówieśników wcale nierzadko demonstrują różnego rodzaju zachowania agresywne.

Ciekawym poznawczo, ale również z perspektywy możliwości poprawy stanu bezpieczeństwa w szkole, może być badanie sposobów radzenia sobie przez uczniów z zagrożeniami. Jednym z takich sposobów jest zwracanie się do innych osób o pomoc w sytuacji zagrożenia, co wiąże się z zaufaniem do instytucjonalnych i nieformalnych przedstawicieli szkoły oraz środowiska pozaszkolnego [Sztompka 2009, ss. 318–324].

Wykres 8. Osoby, do których zwróciliby się badani w sytuacji zagrożenia ich bezpieczeństwa



Źródło: opracowanie własne.

Na wykresie 8 prezentowany jest procentowy rozkład odpowiedzi respondentów na pytanie o to, do kogo zwróciliby się w sytuacji zagrożenia ich bezpieczeństwa. Najwięcej osób wskazało wychowawcę klasy (41%) jako osobę, do której zwrócą się w przypadku zagrożenia bezpieczeństwa, prawie tyle samo badanych (40%) skierowałoby prośbę o pomoc do kolegów/koleżanek (w tym przypadku częściej wskazywali na kolegów uczniowie – prawie 44% z nich – niż uczennice – niespełna 39% z nich – tabela 4). Raczej należało oczekiwać, że na tym etapie rozwoju psychicznego i społecznego (końcowa faza kształcenia w szkole średniej) młodzież będzie oczekiwała wsparcia w zakresie bezpieczeństwa przede wszystkim wśród rówieśników. Uzyskane w trakcie badań dane nie dają wystarczających

podstaw do wyciągania wielu wniosków, np. czy grupy edukacyjne/klasy szkolne są wystarczająco zintegrowane. Niemniej można zauważyć, że w stosunku do podmiotów instytucjonalnych środowiska szkolnego, czyli wychowawców klasy i pedagogów szkolnych łącznie miało zaufanie 51% uczniów (częściej były to uczennice – prawie 53% niż uczniowie – prawie 46% uczniów), prawdopodobnie ma to ścisły związek z oczekiwaniami badanych, że to przede wszystkim szkoła jako instytucja ma zapewnić im bezpieczeństwo oraz z przypisywaniem wychowawcom i pedagogom szkolnym atrybucji sprawczych rozwiązywania sytuacji kryzysowych [Kubacka-Jasiecka 2010, ss. 368–377].

Tabela 4. Zaufanie respondentów (w zależności od ich płci) do osób z środowiska szkolnego w związku z sytuacją zagrożenia

Osoby do których zwróciliby się badani w sytuacji zagrożenia ich bezpieczeństwa N=171	Kobieta			Mężczyzna			Razem	
	n	% z liczebności	% z płci	N	% z liczebności	% z płci	n	%
Wychowawca klasy	50	29,24	43,86	20	11,69	35,09	70	40,93
Pedagog szkolny	10	5,85	8,77	6	3,51	10,53	16	9,36
Kolega/koleżanka	44	25,73	38,60	25	14,62	43,86	69	40,35
Inna osoba	10	5,85	8,77	6	3,51	10,53	16	9,36
Ogółem	114	66,67	100	57	33,33	100	171	100

Źródło: opracowanie własne.

Deklaracje uczniów związane ze współuczestnictwem w kształtowaniu bezpieczeństwa

Współcześnie można wyraźnie dostrzec, że „bezpieczeństwo" to przede wszystkim pewien stan i proces. Oznacza to, że bezpieczeństwo jako stan ma charakter tymczasowy i cechuje się dużą dynamiką. Dlatego też zapewnianie bezpieczeństwa jest procesem ciągłym i wymaga zaangażowania wielu podmiotów, od pojedynczego człowieka poprzez różnorakie grupy społeczne, aż do państwa. Inną przesłanką do zbadania deklaracji maturzystów dotyczących ich gotowości do ewentualnego współuczestnictwa w działaniach na rzecz bezpieczeństwa, było określanie go jako „dobra wspólnego". Można również nazwać je „dobrem publicznym" – czyli

ogólnodostępnym, które służy wszystkim, stanowiąc pozytywną wartość. Z tych względów podjęto próbę zbadania świadomości, wiedzy i nabytego przez respondentów doświadczenia życiowego w kontekście kształtowania bezpieczeństwa.

W nawiązaniu do opisywanych w podrozdziale trzecim dwóch perspektyw czasowych (całożyciowej i epizodycznej) zmienności poczucia bezpieczeństwa i znaczenia wiedzy w zdolności dokonywania adekwatnych ocen, wymieniane w literaturze przedmiotu [m.in. Dziurzyński, Sawicki 2009, ss. 8–9; Marciniak 2009, ss. 60–61; Strumska-Cylwik 2011, s. 41; Zaleski 1991, ss. 128, 225; Moczuk 2009, s. 43] subiektywne czynniki określające życie jednostki jako bezpieczne, można podzielić na kilka wzajemnie zależnych grup:

1) poczucie stabilizacji życiowej, możliwość jej przewidzenia, co związane jest niezwykle silnie z odczuwaniem sensu własnego życia oraz posiadaniem planów i perspektyw życiowych, ale jednocześnie identyfikowanie istniejących realnych zagrożeń dla planów życiowych. W całożyciowej perspektywie na dynamikę poczucia bezpieczeństwa wpływa odczuwanie w przestrzeni społecznej istnienia norm moralnych i prawnych odnoszących się zwłaszcza do trudnej w określeniu sprawiedliwości, ładu i porządku. Maturzyści to część społeczeństwa, która w sensie biologicznym (zbliżony wiek), prawnym stanowi jego dorosłą część, ale pozostaje w stadium przejściowym pomiędzy okresem dzieciństwa a dorosłością (brak samodzielności ekonomicznej i społecznej), co powoduje u młodzieży na tym etapie życia uczucie niepewności i dezorientacji;

2) dobre relacje i silne więzi z bliskimi (m.in. rodzina, krewni) i określonymi kręgami społecznymi. Bezpieczeństwo jednostki i, co za tym idzie, poczucie bezpieczeństwa, w znacznej mierze zależą od bezpieczeństwa grupy społecznej, bezpieczeństwa lokalnego, bezpieczeństwa państwa i bezpieczeństwa międzynarodowego. W końcowej fazie przechodzenia od okresu dzieciństwa do dorosłości, młodzież w większym stopniu niż w środowisku rodzinnym [Szewczuk 2010, ss. 143–162; Kawula 2009, s. 210] i w szkole jako instytucji dydaktyczno-wychowawczej [Wilski 2011, s. 143], poszukuje możliwości zaspokojenia potrzeb psychicznych i społecznych w grupie rówieśniczej, m.in. poczucia pewności, społecznego uznania, afiliacji, zrozumienia, co zapewnia poczucie bezpieczeństwa;

3) poczucie poinformowania, rozumiane jako nabycie usystematyzowanej wiedzy o bezpieczeństwie w toku edukacji dla bezpieczeństwa, organizowanej przede wszystkim w szkole, ale też chodzi tutaj o dostęp i otrzymywanie bieżących informacji o stanie bezpieczeństwa, udostępnianych przez media i instytucje odpowiedzialne za zapewnianie bezpieczeństwa.

Tak rozumiane oddziaływanie wiadomości, szerzej – wiedzy – na poczucie bezpieczeństwa sprawia że wiedza funkcjonuje w umiejętnościach i cenionych wartościach. Przy czym umiejętności obejmują zarówno posługiwanie się konkretnymi, względnie prostymi w obsłudze środkami zapewniającymi bezpieczeństwo, jak też zastosowanie wiadomości w sytuacjach zagrożenia bezpieczeństwa.

Wiadomości i umiejętności w obszarze bezpieczeństwa to niewyłącznie wiedza deklaratywna (wiedza „że") i proceduralna (wiedza „jak") oraz wiedza kontekstowa (wiedza „kiedy i dlaczego"), są one też uobecnione w wartościach i postawach, wyrażających się w aktywnym kształtowaniu bezpieczeństwa, przynajmniej deklarowanym. Opinie respondentów o udziale poszczególnych źródeł wiedzy o współczesnych zagrożeniach, uzyskanej w szkole, zestawiono w tabeli 5.

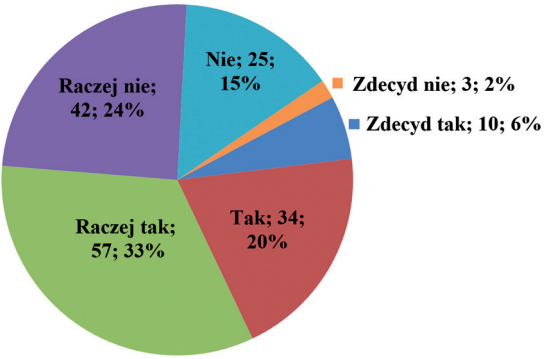
Tabela 5. Liczbowy i procentowy udział źródeł uzyskanej w szkole wiedzy o współczesnych zagrożeniach (badani mogli wskazać maksymalnie dwie odpowiedzi)

Źródła uzyskanej w szkole wiedzy o współczesnych zagrożeniach N=171	n	Procent odpowiedzi	Procent przypadków
Zajęcia przedmiotowe	87	37,02	50,88
Zajęcia z udziałem wychowawcy klasy	57	24,26	33,33
Inne zajęcia/spotkania	91	38,72	53,22
Razem	235	100,00	137,43

Źródło: opracowanie własne.

Wiedza nabywana w ramach systematycznej edukacji przedmiotowej (edukacja dla bezpieczeństwa) została wskazana w prawie 51% przypadków, jeszcze nieco większe znaczenie uczniowie przypisali innym zajęciom i spotkaniom organizowanym w szkole (53% przypadków) i poza nią. Były to formy zajęć dotyczące różnych aspektów bezpieczeństwa, w których brali udział m.in. funkcjonariusze policji, straży pożarnej, straży miejskiej. Łącząc wiedzę teoretyczną z praktyką, ponad połowa badanych (59% – wykres 9) miała możliwość angażowania się w działalność na rzecz bezpieczeństwa uczniów.

Wykres 9. Możliwość angażowania się respondentów w działalność



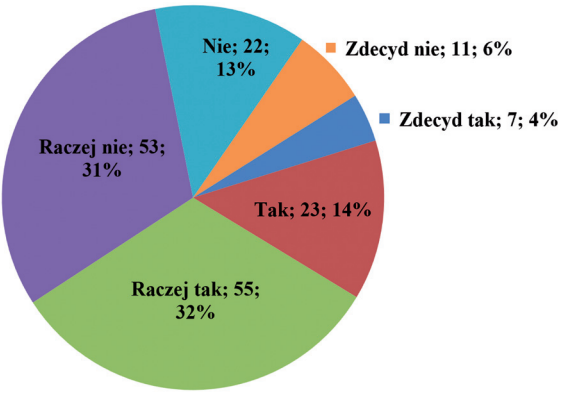
Źródło: opracowanie własne.

Trudno ocenić, w jakim stopniu wiedza i umiejętności nabyte w okresie edukacji w szkole średniej, wpłynęły na zamiar podjęcia studiów związanych z bezpieczeństwem. Na deklaracje uczniów można spojrzeć poprzez trudne do określenia granice wieku i uczestnictwa społecznego. Nadzieje pokładane w edukacji (przynajmniej te deklarowane), sprawiają że już w fazie przeddecyzyjnej maturzyści wykonują mniej czy bardziej konsekwentnie dwie czynności: określają problem do rozwiązania (czy podejmą studia, czy rozpoczną pracę zawodową, a może jednocześnie będą studiowali i pracowali, w każdym wyborze konieczne jest dookreślenie „jakie?", „jaką?" i „gdzie?"), jak również zbierają informacje o dostępnych możliwościach. Ze względu na złożoność problemu, m.in. potrzebę rozpoznania i powiązania indywidualnych cech osobowości jako predyspozycji zawodowych, pomocne są różne formy orientacji i doradztwa zawodowego [Wilsz 2009, s. 261].

Zamiar dalszej edukacji sprawia, że pełne uczestnictwo w życiu społecznym jest odsuwane w czasie [Karkowska 2010, s. 138], ale jednocześnie poprzez zdobycie odpowiedniego wykształcenia młodzież dąży do poszerzenia wpływu na swoją sytuację i możliwości świadomego kierowania przebiegiem życia. We właściwym procesie decyzyjnym co do dalszej drogi życiowej (w tym wyboru rodzaju studiów), uczniowie ostatniego roku nauki w szkole średniej wyróżniają jedną z możliwych opcji [Nęcka, Orzechowski, Szymura 2008, ss. 584, 585] i stopniowo gromadzą wiedzę na temat wybranej możliwości. Głównym elementem procesu decyzyjnego jest ocena ważności zebranych wcześniej informacji, które w przypadku maturzystów mogą ulec nawet znacznym przewartościowaniom już po egzaminie maturalnym i ponownej ocenie szans realizacji podjętych wcześniej

wyborów. Jednym z deklarowanych wyborów było podjęcie studiów w dziedzinie związanej z bezpieczeństwem. Deklaracje badanych maturzystów zestawiono na wykresie 10.

Wykres 10. Deklarowane podjęcie studiów związanych z bezpieczeństwem



Źródło: opracowanie własne.

Dokładnie połowa respondentów deklaruje (przy największym udziale odpowiedzi „raczej tak" – 32%), że podejmie studia z zakresu bezpieczeństwa. Nieco częściej taką gotowość zgłaszali uczniowie liceów ogólnokształcących (50,81% z rodzajów szkoły) niż uczniowie technikum (46,81% z rodzajów szkoły) – tabela 6.

Tabela 6. Deklarowane podjęcie studiów związanych z bezpieczeństwem w zależności od rodzaju szkoły średniej

Podjęcie studiów związanych z bezpieczeństwem N=171	LO		Technikum		Łącznie badani	
	n	%	n	%	n	%
Skumulowane odpowiedzi „zdecydowanie tak", „tak", „raczej tak"	63	z licz. 74,12 z rodz. szkoły 50,81	22	z licz. 25,88 z rodz. szkoły 46,81	85	49,71
Skumulowane odpowiedzi „raczej nie", „nie", „zdecydowanie nie"	61	z licz. 70,93 z rodz. szkoły 49,19	25	z licz. 29,07 z rodz. szkoły 53,19	86	50,29

Źródło: opracowanie własne.

Pełniejszy obraz deklaracji wyboru studiów związanych z bezpieczeństwem ukazują wyliczenia zgromadzone w tabeli 7, obrazujące zależność zadeklarowanych wyborów od profilu kształcenia. Zdecydowanie największy procentowy udział skumulowanych odpowiedzi pozytywnych (86,49%) był dokonany przez uczniów klas mundurowych, na drugim miejscu, lecz już znacznie mniej (54,55%) takich deklaracji złożyli uczniowie ogólnego profilu kształcenia. Udziały skumulowanych pozytywnych deklaracji respondentów profilu matematyczno-fizycznego, biologiczno-chemicznego i innych są na zbliżonym poziomie (odpowiednio: 40%, 41,67% i 37,68%). Należy jednak mieć na uwadze, iż zarówno w przypadku skumulowanych deklaracji pozytywnych, jak i negatywnych, najczęściej (wykres 10) deklarowano „raczej tak" (32%) i „raczej nie" (31%).

Tabela 7. Deklarowane podjęcie studiów związanych z bezpieczeństwem w zależności od profilu kształcenia

Deklaracja podjęcia studiów w dziedzinie bezpieczeństwa N=171	Profil kształcenia										Razem	
	Ogólny		Matemat. - fizyczny		Biologiczno - chemiczny		Klasa mundurowa		Inny			
	n	%	n	%	n	%	n	%	n	%	n	%
Tak - skumulowane odpowiedzi „zdecydowanie tak", „tak", „raczej tak"	6	z licz. 6,97 z profilu 54,55	12	z licz. 13,95 z profilu 40,00	10	z licz. 11,63 z profilu 41,67	32	z licz. 37,21 z profilu 86,49	26	z licz. 30,23 z profilu 37,68	86	50,3
Nie - skumulowane odpowiedzi „raczej nie", „nie", „zdecydowanie nie"	5	z licz. 5,81 z profilu 45,45	18	z licz. 21,18 z profilu 60,00	14	z licz. 16,47 z profilu 58,33	5	z licz. 5,88 z profilu 13,51	43	z licz. 50,59 z profilu 62,32	85	49,7
Ogółem n %	11	6	30	18	24	14	37	22	69	40	171	100

Źródło: opracowanie własne.

Wybór kierunku studiów przez maturzystów jest poprzedzany analizą zarówno własnych predyspozycji, niezbędnego wysiłku, jak też czynników zewnętrznych (trudność danego kierunku studiów, perspektywy pracy zawodowej i wiele innych uwarunkowań). Niewątpliwie znaczącym elementem tego rodzaju analiz i dokonywanych wyborów są wybrane na poziomie edukacji w szkole średniej profile kształcenia. Bardzo wyraźnie widoczne było to w przypadku uczniów klas mundurowych, pośród których prawie 60% deklarujących podjęcie studiów związanych z bezpieczeństwem, wskazało odpowiedź „zdecydowanie tak" i „tak".

Deklaracje maturzystów są bezpośrednio związane z ich aspiracjami, dążeniami i planami na przyszłość. Trudno jednoznacznie ocenić – ze względu chociażby na dynamikę zmian społeczno-ekonomicznych, procesy globalizacji, jak i złożoność badania problematyki współczesnej młodzieży – jaka jest hierarchia cenionych przez nich wartości i związanych z nimi aspiracji. Dla celów poznawczych wymienia się [Karkowska 2010, s. 155] m.in.:

1) aspiracje oświatowe (mądrość, wiedza, inteligencja, rozwój zainteresowań);

2) aspiracje zawodowo-bytowe (sposób życia, jego poziom, pozycja społeczna i zawodowa, praca zgodna z predyspozycjami osobowościowymi, zainteresowaniami, sposoby spędzania czasu wolnego);

3) aspiracje do podmiotowości (wpływ starań i wysiłków na życie).

Na aspiracje uczniów wpływają własne plany, opinie rodziny, media, rynek pracy, ale także szkoła [Karpińska 2003, s. 13], w której edukacja powinna przywracać człowiekowi możliwość decydowania o swoim losie. W tym celu szkołę średnią i wyższą należy traktować jako etapy edukacji przez całe życie.

Zakończenie

Dynamiczny rozwój cywilizacyjny skutkuje wzrostem liczby czynników przyczyniających się do rozwoju wielu zagrożeń. Szkoła stanowi drugie, po rodzinie, środowisko wychowawcze w życiu człowieka. Jest podstawową jednostką oświatowo-wychowawczą w systemie edukacji. W oparciu o zrealizowany projekt badawczy, zasadnym jest stwierdzenie, że bezpieczeństwo i poczucie bezpieczeństwa należą do kluczowych obszarów środowiska szkolnego. Przypadki zagrożeń, chociaż nie występowały nagminnie, były sygnalizowane przez maturzystów. Ponadto przeprowadzone badanie ankietowe pozwala na sformułowanie poniższych wniosków:

1. Poczucie bezpieczeństwa w diagnozowanych szkołach kształtowało się na wysokim poziomie. Było ono nawet wyższe niż poczucie bezpieczeństwa w wymiarze krajowym i lokalnym. Zatem im bliższe było otoczenie społeczne badanych (kraj, społeczność lokalna, szkoła), tym większe poczucie bezpieczeństwa. Warto podkreślić, że badane cechy demograficzne uczniów nie miały większego znaczenia dla ich wskazań.

2. Spośród wielu czynników o różnym charakterze ankietowani najczęściej przyznawali najwyższe znaczenie relacjom nauczyciele-uczniowie oraz uczniowie-uczniowie. Pozostałym czynnikom przypisywano dużo mniejsze znaczenie (m.in. monitoring wewnętrzny szkoły, profilaktyka czy system wchodzących do szkoły). Zdecydowanie najmniejsze znaczenie miał monitoring wokół szkoły, dyscyplinujące działania nauczycieli oraz działania samorządów uczniowskich.

3. Dominującym zagrożeniem w opiniach respondentów okazały się przede wszystkim przekleństwa i wyzwiska. Kolejnymi zagrożeniami o dwukrotnie mniejszej częstotliwości były: psychiczne znęcanie się oraz popychanie lub bicie. W najmniejszym stopniu maturzyści obawiali się niszczenia cudzej własności, różnego rodzaju środków odurzających, a także wymuszania pieniędzy.

4. Wyniki uzyskane z przeprowadzonych badań pozwalają sformułować tezę, iż obecnie maleje znaczenie funkcji opiekuńczej szkoły (w zależności od poziomu edukacji), a zdecydowanie wzrasta oczekiwanie zapewnienia bezpieczeństwa społeczności szkolnej. Potwierdzeniem słuszności tej tezy są wyniki dotyczące zaufania do uczniów i wychowawców w sytuacji wystąpienia zagrożenia.

W kontekście badanej problematyki ważna była też deklaracja ponad połowy ankietowanych, związana z ich gotowością do współuczestnictwa w kształtowaniu bezpieczeństwa. Świadczyłoby to o rozumieniu jego istoty i znaczenia przez maturzystów.

Bibliografia

Aronson E., Wilson T.D., Akert R.M. (2006), *Psychologia społeczna*, Zysk i S-ka Wydawnictwo, Poznań.

Brzeziński M. (red.) (2009), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia,* Elipsa, Warszawa.

Dziurzyński K., Sawicki A. (2009), *Doświadczanie bezpieczeństwa w wymiarze lokalnym* [w:] W. Fehler (red.), *Bezpieczeństwo w środowisku lokalnym*, Arte, Warszawa.

Dunaj B. (red.) (2007), *Uniwersalny słownik język polskiego*, Reader's Digest, Warszawa.

Encyklopedia Popularna (1998), t. 1, PWN, Warszawa.

Karkowska M. (2010), *Socjologia wychowania. Wybrane elementy. Mechanizmy socjalizacji i edukacja szkolna*, Wydawnictwo Akademii Humanistyczno-Ekonomicznej, Łódź.

Karpińska A. (red.) (2003), *Edukacyjne problemy globalizacji,* Trans Humana, Białystok.

Kawula S. (2009), *Rodzina a start społeczny i edukacyjny młodych pokoleń* [w:] S. Kawula, J. Brągiel, A.W. Janke, *Pedagogika rodziny. Obszary i panorama problematyki*, Wydawnictwo Adam Marszałek, Toruń, ss. 195–217.

Konieczny J. (2005), *Bezpieczeństwo uczelni – bezpieczeństwo szkoły*, Krakowskie Towarzystwo Edukacyjne, Kraków.

Konarzewski K. (red.) (2005), *Sztuka nauczania. Szkoła*, Wydawnictwo Naukowe PWN, Warszawa.

Konstytucja RP z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. nr 78 poz. 483).

Kubacka-Jasiecka D. (2010), *Interwencja kryzysowa. Pomoc w kryzysach psychologicznych*, WAiP, Warszawa.

Kupisiewicz C. (2005), *Podstawy dydaktyki*, WSiP, Warszawa.

Marciniak E.M. (2009), *Psychologiczne aspekty poczucia bezpieczeństwa* [w:] S. Sulowski, M. Brzeziński (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Dom Wydawniczy ELIPSA, Warszawa.

Matusewicz Cz. (2006), *Wprowadzenie do psychologii*, Vizja Press&IT, Warszawa.

McWhirter E.H., McWhirter J.J., McWhirter A.M. (2001), *Zagrożona młodzież*, Wyd. PARPAMEDIA, Warszawa.

Moczuk E. (2009), *Socjologiczne aspekty bezpieczeństwa lokalnego*, Wyd. URz, Rzeszów.

Nęcka E., Orzechowski J., Szymura B. (2008), *Psychologia poznawcza*, Akademica Wydawnictwo SWPS, Wydawnictwo Naukowe PWN, Warszawa.

Niemczyński A. (1988), *Procesy rozwojowe człowieka w pełnym cyklu życia indywidualnego* [w:] M. Tyszkowa (red.), *Rozwój psychiczny człowieka w ciągu życia. Zagadnienia teoretyczne i metodologiczne*, Państwowe Wydawnictwo Naukowe, Warszawa.

Obuchowska I. (2009), *Problemowe zachowania uczniów* [w:] K. Kruszewski (red.), *Sztuka nauczania. Czynności nauczyciela*, Wydawnictwo Naukowe PWN, Warszawa.

Ratajek Z. (2007), *Relacja uczeń-nauczyciel w szkole – obszary napięć i współpracy* [w:] I. Pufal-Struzik (red.), *Agresja i przemoc w szkole. Przyczyny, rozpoznawanie, zapobieganie*, Wydawnictwo Pedagogiczne ZNP Spółka z o.o., Kielce.

Strumska-Cylwik L. (2011), *Doświadczenia komunikacyjne a poczucie bezpieczeństwa w kontekście wybranych aspektów komunikowania wzajemnego* [w:] J. Podgórecki, A. Dąbrowski, K. Czerwiński, *Bezpieczeństwo w perspektywie komunikowania społecznego i jego edukacyjne uwarunkowania*, Wydawnictwo Adam Marszałek, Toruń.

Sulowski S., Brzeziński M. (red.) (2009), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Elipsa, Warszawa.

Szewczuk K. (2010), *Wybrane zagadnienia pedagogiki rodziny*, Wyższa Szkoła Filozoficzno-Pedagogiczna „Ignatianum", Wydawnictwo WAM, Kraków.

Sztompka P. (2009), *Socjologia. Analiza społeczeństwa*, Wydawnictwo Znak, Kraków.

Szweda E. (2016), *Bezpieczeństwo społeczności lokalnych. Najbliżej człowieka*, Difin S.A., Warszawa.

Wilski M. (2011), *Adaptacja uczniów do warunków szkoły* [w:] S. Kowalik (red.), *Psychologia ucznia i nauczyciela*, Wydawnictwo Naukowe PWN, Warszawa.

Wilsz J. (2009), *Teoria pracy. Implikacje dla pedagogiki pracy*, Oficyna Wydawnicza „Impuls", Kraków.

Zaleski Z. (1991), *Psychologia zachowań celowych*, PWN, Warszawa.

Ustawa z dnia 7 września 1991 r. *o systemie oświaty* (Dz. U. z 2018 r. poz. 1457, 1560).

https://cke.gov.pl/images/_KOMUNIKATY/20180412%20Egzamin%20maturalny%202018.pdf.

https://bezpiecznaszkola.men.gov.pl/bezpieczna-szkola-zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizycznego-i-cyfrowego-uczniow/.

Anna Kosieradzka | Anna.Kosieradzka@pw.edu.pl
Politechnika Warszawska, Wydział Zarządzania

Justyna Smagowicz | Justyna.Smagowicz@pw.edu.pl
Politechnika Warszawska, Wydział Zarządzania

Michał Wiśniewski | Michal.Wisniewski@pw.edu.pl
Politechnika Warszawska, Wydział Zarządzania

Struktura repozytorium dobrych praktyk wykorzystywanych w publicznym zarządzaniu kryzysowym

Wprowadzenie

Dobre praktyki towarzyszą działaniom podejmowanym przez organizację we wszystkich obszarach zarządzania. Stanowią one dorobek nauk o zarządzaniu, wypracowany przez naukowców i praktyków w celu poprawy skuteczności i efektywności funkcjonowania organizacji.

W wyniku badań prowadzonych w ramach projektu rozwojowego[1], poszukując koncepcji, metod i technik do zastosowania w publicznym zarządzaniu kryzysowym, zauważono dwojakie rozumienie pojęcia dobrych praktyk. Z jednej strony dobre praktyki definiowane są jako zbiór metod i technik możliwych do

[1] Publikacja bazuje na wynikach z analiz zrealizowanych w toku projektu pt. „Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej RP oraz w jednostkach organizacyjnych KSRG", realizowanego w ramach konsorcjum Politechnika Warszawska Wydział Zarządzania oraz Medcore Sp. z o.o., konkurs nr 7/2015.

zastosowania przy rozwiązywaniu danego problemu decyzyjnego, przy czym często narzędzia te są znane i stosowane również w różnych obszarach zarządzania, nie tylko w zarządzaniu kryzysowym. Drugie podejście przedstawia dobre praktyki jako wzorce działań – gotowe rozwiązania, możliwe do wdrożenia w przypadku wystąpienia sytuacji kryzysowej, których zastosowanie pozwoli osiągnąć zadowalające rezultaty, a wiedza ta jest czerpana z dotychczasowych doświadczeń i obserwacji przebiegu sytuacji kryzysowych i zastosowanych w nich rozwiązań. W tym rozumieniu dobre praktyki nie obejmują zestawu metod i technik wspomagających analizę problemu, ocenę i wybór najlepszego rozwiązania, lecz przedstawiają zestaw konkretnych zadań, koniecznych do podjęcia przez powołane do tego podmioty [Wiśniewski, Kunikowski, Kisilowski 2017].

Niniejsze opracowanie skupia się na pierwszym z powyższych podejść, to znaczy, na dobrych praktykach, rozumianych jako metody i techniki stosowane w rozwiązaniu problemu decyzyjnego z obszaru zarządzania kryzysowego.

W obszarze publicznego zarządzania kryzysowego obowiązują przepisy regulujące działania podejmowane przez poszczególne jednostki administracji publicznej, jednakże w przepisach tych istnieje duża dowolność w zakresie doboru metod i technik stosowanych do osiągania celów wyznaczonych w ramach procesów planowania cywilnego i zarządzania kryzysowego [Tyburska 2009, s. 96; Krupa, Wiśniewski 2015, s. 94; Lidwa 2015, ss. 165–176]. Z jednej strony działania prowadzone w ramach obydwu procesów są obarczone dużą odpowiedzialnością za bezpieczeństwo narodowe, a jednocześnie z drugiej strony nie została zdefiniowana baza wiedzy klasyfikująca narzędzia wspomagające ich realizację.

Celem niniejszego artykułu jest zaproponowanie struktury repozytorium dobrych praktyk, które będzie można zastosować w publicznym zarządzaniu kryzysowym. W ramach opracowania autorzy przedstawią strukturę repozytorium dobrych praktyk opracowaną na potrzeby publicznego zarządzania kryzysowego, przykład charakterystyki metody według wzorca zaimplementowanego w repozytorium oraz rekomendacje technologii wykonania repozytorium.

Metoda badawcza

Koncepcja repozytorium dobrych praktyk na potrzeby publicznego zarządzania kryzysowego opiera się na dwóch filarach. Jednym z nich jest tzw. metryka opisu dobrej praktyki, a drugim – wieloprzekrojowa klasyfikacja zbioru dobrych praktyk.

W celu identyfikacji najlepszych praktyk dedykowanych dla publicznego zarządzania kryzysowego skorzystano z opracowań zawierających klasyfikacje narzędzi stosowanych w różnych obszarach nauk o zarządzaniu. Były to przede wszystkim:

- klasyfikacja metod i technik organizatorskich [Lis 1999],
- klasyfikacja metod stosowanych w procesie oceny ryzyka [ISO 31010],
- klasyfikacja norm i standardów z zakresu zarządzania ryzykiem [Kosieradzka, Zawiła-Niedźwiecki 2016, ss. 19–34],
- klasyfikacja metod wykorzystywanych w procesie foresightu, dedykowanych do wykorzystania w procesie zarządzania ryzykiem [Skomra 2015, ss. 48–81],
- klasyfikacja metod twórczego myślenia [Kosieradzka 2013],
- wykaz dobrych praktyk stosowanych w metodykach zagranicznych [Wiśniewski, Ostrowska 2016, ss. 111–123].

Każda metoda została scharakteryzowana w ujednolicony sposób, obejmujący:

- nazwę metody,
- opis metody oraz możliwych zastosowań,
- etapy metody,
- procedurę stosowania,
- narzędzia wspomagające (np. komputerowe),
- przynależność danej metody do poszczególnych klasyfikacji,
- wymagania wstępne,
- odwołania do źródeł omawiających metodę,
- ocenę użyteczności danej metody w ramach wskazanego obszaru.

W celu identyfikacji przekrojów klasyfikacyjnych i wymiarów w obrębie poszczególnych przekrojów dokonano analizy dokumentów normatywnych związanych z procesem planowania cywilnego i zarządzania kryzysowego. Wyniki uzyskane w ramach realizowanego projektu rozwojowego wskazały, że zostały przyjęte następujące przekroje klasyfikacji dobrych praktyk:

- działania podejmowane w ramach UMOL,
- działania podejmowane w procesie planowania cywilnego,
- działania podejmowane w procesie zarządzania kryzysowego,
- działania podejmowane w procesie zarządzania ryzykiem,
- dojrzałość organizacji w obszarze publicznego zarządzania kryzysowego.

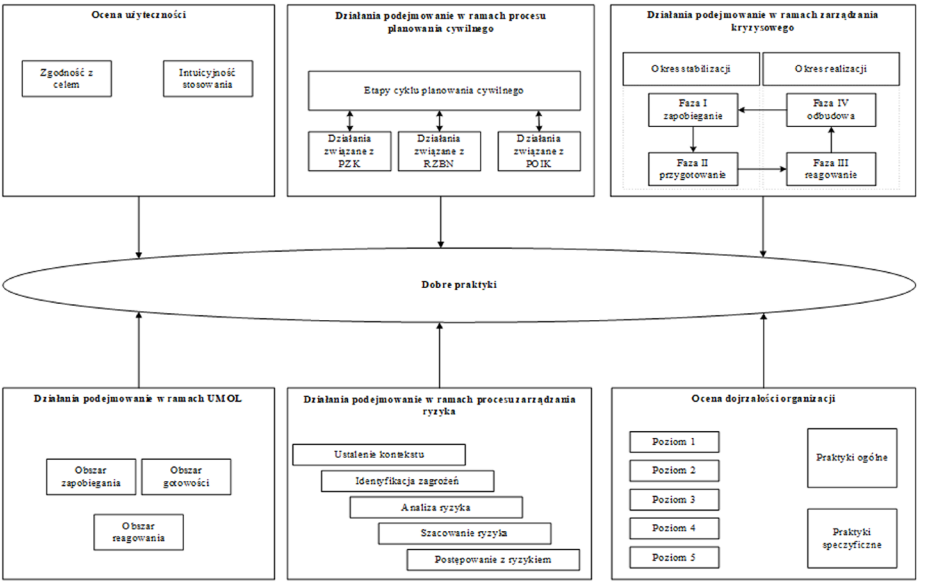
W ramach wskazanych przekrojów określono kluczowe wymiary, stanowiące podstawę opisu dobrej praktyki w ramach klasyfikacji. Wspomniane przekroje klasyfikacji zostały szczegółowo omówione w publikacji [Kosieradzka, Smagowicz, Wiśniewski 2019].

Struktura repozytorium dobrych praktyk dla publicznego zarządzania kryzysowego

Wymiary klasyfikacji dobrych praktyk posłużyły do opracowania struktury repozytorium, skupiającego metody możliwe do wykorzystania w publicznym zarządzaniu kryzysowym (rysunek 1). Podstawowa funkcjonalność repozytorium zakłada, że wybór metody będzie się odbywał poprzez podanie zestawu kryteriów pozwalających na dobranie odpowiedniego narzędzia do założonego celu, np.:

- realizowanego procesu,
- etapu działania w procesie,
- poziomu administracyjnego,
- poziomu dojrzałości organizacji itp.

Rysunek 1. Przekroje klasyfikacji dobrych praktyk występujące w publicznym zarządzaniu kryzysowym



Źródło: [Kosieradzka, Smagowicz, Wiśniewski 2019].

Opis metod według wzorca charakterystyki dobrej praktyki

W dalszej części artykułu przedstawiono opis dwóch wybranych metod zakwalifikowanych jako dobre praktyki w publicznym zarządzaniu kryzysowym. Pierwszą z nich jest metoda wstępnej analizy zagrożeń (ang. *Preliminary Hazard Analysis*), stanowiąca matrycową metodę oceny ryzyka bazującą na określeniu prawdopodobieństwa (wystąpienia szkody) oraz skutku wywołanego rozpatrywanym zagrożeniem. Drugą metodą jest jedna z metod pobudzania kreatywności opracowana przez de Bono – metoda „6 kapeluszy".

Podstawowe charakterystyki metody wstępnej analizy zagrożeń to:

- **Nazwa metody:** Metoda Preliminary Hazard Analysis (PHA),
- **Zakres stosowania:** Metoda umożliwia identyfikację zarówno pojedynczych zagrożeń, jak i rozpatrywanie scenariuszy zdarzeń niekorzystnych dla rozpatrywanego obiektu, np. IK.
- **Etapy metody:** a) określenie przyczyny wystąpienia rozpatrywanego skutku, b) określenie środków kontroli, c) oszacowanie prawdopodobieństwa wystąpienia zagrożenia, d) określenie wpływu zdarzenia na rozpatrywany obiekt, e) określenie poziomu ryzyka.
- **Wskazówki stosowania:** Metoda PHA jest wykorzystywana w sytuacjach, gdy zestaw danych dotyczący procesów realizowanych w przedsiębiorstwie jest niekompletny lub dane nie są szczegółowe. Wyniki metody stanowią wstępny etap dla właściwego oszacowania poziomu ryzyka.
- **Narzędzia wspomagające:** Arkusz kalkulacyjny.
- **Wymagania wstępne:** Brak.
- **Źródło:** Kosieradzka A., Zawiła-Niedźwiecki J. (red.) (2016), *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym*.

W tabeli 1 został przedstawiony opis metody wstępnej analizy zagrożeń zgodnie z przyjętym wzorcem charakterystyki dobrej praktyki.

Tabela 1. Przykład opisu metody PHA zgodnie z wzorcem opisu dobrych praktyk

Nazwa wymiaru	Opis wymiaru wymiar	Atrybut opisu	Wartość atrybutu
UMOL	Etapy działania podejmowane w UMOL	Obszar zapobiegania	TAK
Działania podejmowane w ramach zarządzania kryzysowego	Okresy działań podejmowanych w procesie zarządzania kryzysowego	Okres stabilizacji	TAK
	Fazy działania podejmowanie w procesie zarządzania kryzysowego	Faza zapobieganie	TAK
		Faza przygotowanie	TAK
Działania podejmowane w ramach procesu planowania cywilnego	Poziom działań podejmowanych w procesie planowania cywilnego	Poziom powiatowy	TAK
		Poziom gminny	TAK
		Poziom operatora IK	TAK
	Etapy działań podejmowane w procesie planowania cywilnego	Analizowanie	TAK
	Rodzaje dokumentów powstające w ramach procesu planowania cywilnego	Plan Zarządzania Kryzysowego	TAK
		Plan Ochrony Infrastruktury Krytycznej	TAK
		Raport o Zagrożeniach Bezpieczeństwa Narodowego	TAK
	Elementy Planu Zarządzania Kryzysowego	Charakterystyka zagrożeń	TAK
		Zestawienie sił i środków	TAK
	Elementy Raportu o Zagrożeniach Narodowych	Zagrożenia	TAK
		Analiza skutków	TAK
		Ocena ryzyka	TAK
		Zapobieganie	TAK
		Przygotowanie	TAK
	Elementy Raportu Cząstkowego o Zagrożeniach Bezpieczeństwa Narodowego	Zagrożenia	TAK
		Zapobieganie	TAK
		Przygotowanie	TAK
		Reagowanie	NIE
		Dane historyczne	NIE
	Elementy Planu Ochrony Infrastruktury Krytycznej	Dane ogólne	TAK
		Dane IK	TAK
		Charakterystyka zagrożeń	TAK

Nazwa wymiaru	Opis wymiaru wymiar	Atrybut opisu	Wartość atrybutu
Ocena dojrzałości organizacji	Wymiar opisujący poziom dojrzałości podmiotu	Poziom 1	TAK
		Poziom 2	TAK
	Charakterystyka zasięgu metod i technik uznanych za dobre praktyki	Praktyka ogólna	TAK
Działania podejmowane w ramach procesu zarządzania ryzykiem	Etapy działań występujące w procesie zarządzania ryzykiem	Ustalenie kontekstu	TAK
		Identyfikacja zagrożeń	TAK
	Działania podejmowane w ramach etapów procesu zarządzania ryzykiem	Opis charakterystyki obiektu	TAK
		Określenie zagrożeń	TAK
		Ustalenie powiązań	TAK
		Ocena skutków	TAK
		Ocena prawdopodobieństwa	TAK
		Obliczenie wartości ryzyka	TAK
		Wyznaczenie poziomu ryzyka	TAK
		Plan ciągłości działania	TAK
Ocena użyteczności	Parametry służące subiektywnej ocenie użyteczności metody lub techniki	Zgodność z celem	5
		Intuicyjność stosowania	4

Źródło: opracowanie własne.

Dane dotyczące charakterystyki rozpatrywanej metody pozwalają użytkownikowi na zapoznanie się z podstawowymi wiadomościami, które umożliwiają zastosowanie metody. Z kolei dane zebrane w tabeli 1 pozwalają określić, dla jakich elementów procesu planowania cywilnego ratowniczego lub zarządzania kryzysowego metoda jest rekomendowana.

Z rozpatrywanego przykładu wynika, że metoda PHA może być stosowana w ramach:

- UMOL w obszarze zapobiegania zagrożeniom,
- procesu zarządzania kryzysowego do działań podejmowanych w okresie stabilizacji w obu jego fazach,
- procesu planowania cywilnego na poziomie operatora IK, gminy i powiatu do działań analitycznych związanych z przygotowaniem Planu Zarządzania Kryzysowego (w obszarze: ustalania charakterystyki zagrożeń, wskazywania zestawu sił i środków reakcji na zagrożenie), Planu Ochrony IK (w obszarze: zebrania danych ogólnych, danych dotyczących IK, charakterystyki zagrożeń) oraz Raportu

o Zagrożeniach Bezpieczeństwa Narodowego (w obszarze: wskazywania zagrożeń, analizy ich skutków, oceny ryzyka, rozpoznania działań zapobiegawczych i przygotowawczych na wypadek wystąpienia zagrożenia),

- procesu zarządzania ryzykiem na etapie identyfikacji podmiotu chronionego oraz możliwych do wystąpienia zagrożeń, a następnie określenia związanego z nimi ryzyka.
- ciągłego doskonalenia, w postaci budowania dojrzałości organizacji z wykorzystaniem danej metody przez wybranych pracowników.

Ponadto metoda PHA należy do grupy metod ogólnych pochodzących z obszaru metod stosowanych do zarządzania ryzykiem. Może być stosowana do ustalenia kontekstu, identyfikacji zagrożeń, opisu charakterystyki obiektu, ustalenia powiązań zagrożeń, oceny skutków i prawdopodobieństwa ich wystąpienia oraz wyznaczenia poziomu ryzyka w ramach procesu zarządzania ryzykiem.

Średnia ocena użyteczności metody PHA w obszarze zgodności z celem wynosi 5, co jest maksymalnym wynikiem, a ocena użyteczności w obszarze intuicyjności stosowania wynosi 4, co sugeruje, że stosowanie metody nie sprawia kłopotów użytkownikom.

W ramach realizowanego projektu badawczego autorzy opracowania dokonali charakterystyki wszystkich metod rekomendowanych przez normę ISO 310010 zgodnie z wzorcem charakterystyki dobrej praktyki. Materiał ten stanowi wkład merytoryczny gotowy do implementacji w repozytorium dobrych praktyk z zakresu publicznego zarządzania kryzysowego.

Kolejną grupą metod możliwą do zaimplementowania we wspomnianym repozytorium jest metoda „6 kapeluszy".

Podstawowe charakterystyki metody „6 kapeluszy" to:

- **Nazwa metody:** Metoda „6 kapeluszy".
- **Zakres stosowania:** Metoda umożliwia identyfikację zarówno pojedynczych zagrożeń, jak i rozpatrywanie scenariuszy zdarzeń niekorzystnych dla rozpatrywanego obiektu.
- **Etapy metody:** a) określenie możliwych zagrożeń, b) określenie skutków wystąpienia zagrożeń, c) określenie powiązań pomiędzy zagrożeniami oraz scenariuszy zdarzeń, d) wybór możliwych rozwiązań.
- **Wskazówki stosowania:** Metoda „6 kapeluszy" umożliwia spojrzenie na dany problem z różnych perspektyw, w związku z tym powinna być stosowana do identyfikacji i systematyzacji zagrożeń oraz określenia możliwych skutków jej wystąpienia. Wyniki metody stanowią wstępny etap dla właściwego oszacowania poziomu ryzyka.

- **Narzędzia wspomagające:** Arkusz kalkulacyjny.
- **Wymagania wstępne:** Brak.
- **Źródło:** Kosieradzka A. (2013), *Metody i techniki pobudzania kreatywności w organizacji i zarządzaniu*.

W tabeli 2 został przedstawiony opis metody „6 kapeluszy" zgodnie z przyjętym wzorcem charakterystyki dobrej praktyki.

Tabela 2. Przykład opisu metody „6 kapeluszy" zgodnie z wzorcem opisu dobrych praktyk

Nazwa wymiaru	Opis wymiaru wymiar	Atrybut opisu	Wartość atrybutu
UMOL	Etapy działania podejmowane w UMOL	Obszar zapobiegania	TAK
Działania podejmowane w ramach zarządzania kryzysowego	Okresy działań podejmowanych w procesie zarządzania kryzysowego	Okres stabilizacji	TAK
	Fazy działania podejmowanie w procesie zarządzania kryzysowego	Faza zapobiegania	TAK
		Faza przygotowanie	TAK
Działania podejmowane w ramach procesu planowania cywilnego	Poziom działań podejmowanych w procesie planowania cywilnego	Poziom powiatowy	TAK
Działania podejmowane w ramach procesu planowania cywilnego		Poziom gminny	TAK
		Poziom operatora IK	TAK
	Etapy działań podejmowane w procesie planowania cywilnego	Analizowanie	TAK
		Opracowanie planu/ /programu	TAK
	Rodzaje dokumentów powstające w ramach procesu planowania cywilnego	Plan Zarządzania Kryzysowego	TAK
		Plan Ochrony Infrastruktury Krytycznej	TAK
		Raport o Zagrożeniach Bezpieczeństwa Narodowego	TAK

Nazwa wymiaru	Opis wymiaru wymiar	Atrybut opisu	Wartość atrybutu
Działania podejmowane w ramach procesu planowania cywilnego	Elementy Planu Zarządzania Kryzysowego	Charakterystyka zagrożeń	TAK
		Zestawienie sił i środków	TAK
		Określenie trybu i sposobu ogłaszania o zaistnieniu przekroczeń	TAK
	Elementy Raportu o Zagrożeniach Narodowych	Zagrożenia	TAK
		Scenariusze	TAK
		Analiza skutków	TAK
		Zapobieganie	TAK
	Elementy Raportu Cząstkowego o Zagrożeniach Bezpieczeństwa Narodowego	Zagrożenia	TAK
		Zapobieganie	TAK
		Przygotowanie	TAK
	Elementy Planu Ochrony Infrastruktury Krytycznej	Dane ogólne	TAK
		Dane IK	TAK
		Charakterystyka zagrożeń	TAK
		Charakterystyka zależności	TAK
		Warianty działania w sytuacji zagrożenia	TAK
		Warianty zapewnienia ciągłości działania	TAK
		Warianty odtwarzania IK	TAK
Ocena dojrzałości organizacji	Wymiar opisujący poziom dojrzałości podmiotu	Poziom 1	TAK
		Poziom 2	TAK
	Charakterystyka zasięgu metod i technik uznanych za dobre praktyki	Praktyka ogólna	TAK

Nazwa wymiaru	Opis wymiaru wymiar	Atrybut opisu	Wartość atrybutu
Działania podejmowane w ramach procesu zarządzania ryzykiem	Etapy działań występujące w procesie zarządzania ryzykiem	Ustalenie kontekstu	TAK
		Identyfikacja zagrożeń	TAK
		Analiza ryzyka	TAK
		Postępowanie z ryzykiem	TAK
	Działania podejmowane w ramach etapów procesu zarządzania ryzykiem	Opis charakterystyki obiektu	TAK
		Określenie zagrożeń	TAK
		Ustalenie powiązań	TAK
		Ocena skutków	TAK
		Zapobieganie ryzyku	TAK
		Plan ciągłości działania	TAK
Ocena użyteczności	Parametry służące subiektywnej ocenie użyteczności metody lub techniki	Zgodność z celem	4
		Intuicyjność stosowania	3

Źródło: opracowanie własne.

Dane przedstawione w powyższej tabeli wskazują, w których elementach procesu publicznego zarządzania kryzysowego możliwe jest zastosowanie metody „6 kapeluszy". W porównaniu z opisaną wcześniej metodą PHA nie pozwala ona na dokonanie oceny ryzyka pod względem prawdopodobieństwa niekorzystnych skutków czy określenia poziomu ryzyka, jednakże jest użyteczna na etapie ustalania powiązań między zagrożeniami czy określania możliwych ciągów zdarzeń oraz działań zapobiegawczych. Z rozpatrywanego przykładu wynika, że metoda „6 kapeluszy" może być stosowana w ramach:

- UMOL w obszarze zapobiegania zagrożeniom,
- procesu zarządzania kryzysowego do działań podejmowanych w okresie stabilizacji w obu jego fazach,
- procesu planowania cywilnego na poziomie operatora IK, gminy i powiatu do działań analitycznych związanych z przygotowaniem Planu Zarządzania Kryzysowego, Planu Ochrony IK oraz Raportu o Zagrożeniach Bezpieczeństwa Narodowego,

- procesu zarządzania ryzykiem na etapie identyfikacji podmiotu chronionego oraz możliwych do wystąpienia zagrożeń, a następnie określenia działań podejmowanych w ramach postępowania z ryzykiem,
- ciągłego doskonalenia, w postaci budowania dojrzałości organizacji z wykorzystaniem danej metody przez wybranych pracowników.

Średnia ocena użyteczności metody PHA w obszarze zgodności z celem wynosi 4, co oznacza, że może być stosowana w większości jednostek samorządu terytorialnego, a ocena użyteczności w obszarze intuicyjności stosowania wynosi 3, co sugeruje, że użytkownicy metody muszą zapoznać się z warunkami i zasadami stosowania tej metody.

Technologia implementacji repozytorium

Realizacja procesów związanych z publicznym zarządzaniem kryzysowym (planowania cywilnego, ratowniczego i zarządzania kryzysowego), w ramach których powstają Raporty o Zagrożeniach Bezpieczeństwa Narodowego, Plany Zarządzania Kryzysowego i Plany Ochrony IK, jest możliwa bez wsparcia narzędzi informatycznych. Jednak w tym przypadku efektywność procedur, mierzona czasem potrzebnym na ich realizację, będzie niska.

Argumentem przemawiającym za wprowadzeniem systemu informatycznego wspomagającego przygotowanie planów ratowniczych i planów zarządzania kryzysowego jest konieczność budowania bazy wiedzy na temat metod i technik przyspieszających ich powstawanie oraz podnoszących jakość treści w nich zawartych. Dane dotyczące dobrych praktyk powinny pochodzić z wielu źródeł, a ich użyteczność powinna być oceniana przez wielu użytkowników. Zapewni to możliwość porównywania wielu metod i technik stosowanych dla tych samych obszarów działań. Z czasem zebrane oceny pozwolą na wskazanie najskuteczniejszych rozwiązań, zawężając ich zbiór do niezbędnego minimum – wówczas repozytorium może zostać rozbudowane o elementy wymagane do utworzenia systemu eksperckiego [Wiśniewski 2013]. Brak wspólnego narzędzia informatycznego, umożliwiającego przechowywanie tych danych, utrudni ich gromadzenie, co będzie rzutowało na efektywność realizowanych działań w ramach procesu planowania cywilnego, ratowniczego i zarządzania kryzysowego.

W związku z koniecznością wsparcia procesu gromadzenia opisów dobrych praktyk z zakresu planowania cywilnego oraz budowy planów ratowniczych i planów zarządzania kryzysowego narzędziem informatycznym przedstawiono

wymagania niefunkcjonalne[2] (tabela 3) dla projektowanego repozytorium, które warunkują technologie jego implementacji.

Tabela 3. Wykaz wymagań niefunkcjonalnych

Symbol wymagania	Opis wymagania
Dostęp do narzędzia	
WN1	interfejs użytkownika dostępny przez aplikację webową[3]
Skalowalność	
WN2	zapewnienie sprawności i ciągłości działania projektowanego narzędzia informatycznego w sytuacji eksploatacji przez zwiększoną liczbę użytkowników oraz zwalnianie zasobów sprzętowych w sytuacji eksploatacji przez zmniejszoną liczbę użytkowników
WN3	zapewnienie braku pojedynczego punktu awarii systemu – wszystkie elementy infrastruktury powinny być odpowiednio zwielokrotnione
Kompatybilność	
WN4	zgodność narzędzia z popularnymi systemami operacyjnymi Windows 8.1 i nowszymi, Linux, Fedora, Ubuntu, Debian, openSUSE
Dostępność	
WN5	wszystkie elementy aplikacji powinny zapewniać funkcjonowanie aplikacji z dostępnością nie mniejszą niż 98% w ciągu roku
WN6	prace administracyjne powodujące niedostępność aplikacji lub jej części powinny być wykonywane w taki sposób, aby nie uniemożliwiały korzystania z portalu przez użytkowników
WN7	powinno być zapewnione ciągłe (bez konieczności wprowadzania przerw technicznych) działanie całości aplikacji (wszystkich jej komponentów i realizacja wszystkich jej funkcji)

[2] Wymagania niefunkcjonalne dotyczą tego jak budowane narzędzie informatyczne powinno realizować swoje zadania np. opis wymagań dotyczących niezbędnych zasobów informacyjnych, ograniczenia czasowe, wymagania dotyczące niezawodności, wymagania dotyczące bezpieczeństwa, przenośności, współpracy z określonymi narzędziami i środowiskami, zgodności z normami i standardami, a także przepisami prawnymi, w tym dotyczącymi tajności i prywatności itp. [Socha 2010, s. 53].

[3] Program komputerowy, który pracuje na serwerze i komunikuje się poprzez sieć komputerową z hostem użytkownika komputera z wykorzystaniem przeglądarki internetowej użytkownika, będącego w takim przypadku interaktywnym klientem aplikacji internetowej.

Symbol wymagania	Opis wymagania
Bezpieczeństwo	
WN8	wymagania dotyczące bezpieczeństwa dotyczą obszarów: • uwierzytelniania • zarządzania sesją • kontroli dostępu • obsługi błędów i logowania • ochrony danych • bezpieczeństwa komunikacji • bezpieczeństwa http • konfiguracji zabezpieczeń
Integracja	
WN9	zapewnienie możliwości integracji z istniejącymi bazami danych dotyczącymi zdarzeń niekorzystnych, np. bazą danych Państwowej Straży Pożarnej, Centralnej Aplikacji Raportującej.

Źródło: opracowanie własne.

Wymagania niefunkcjonalne, dotyczące skalowalności projektowanego narzędzia informatycznego, sugerują wykorzystanie technologii chmury obliczeniowej (ang. *Cloud Computing* – CC) do implementacji struktury repozytorium.

Ze względu na ułatwienie procesu administrowania narzędziem informatycznym, które ma wspomagać gromadzenie wzorców dobrych praktyk, proponuje się wykorzystanie modelu Software as a Service (SaaS), który umożliwia klientom użytkowanie oprogramowania hostowanego przez dostawcę. Usługobiorca sam decyduje, z jakiego pakietu programów oferowanych przez dostawcę będzie korzystał i w jakim wymiarze funkcjonalnym. Model SaaS umożliwia przedsiębiorcom płacenie tylko za te funkcje oprogramowania, które rzeczywiście eksploatują i ponoszenie opłaty za rzeczywisty czas wykorzystania. Pakiet oprogramowania dedykowany dla klienta funkcjonuje, przy zachowaniu ustalonego w umowie poziomu bezpieczeństwa danych, obok pakietów programowych innych klientów na wspólnym serwerze dostawcy usługi. Usługobiorca ustala liczbę pracowników, którzy mają dostęp do udostępnionych programów. Liczba pracowników i rzeczywisty czas wykorzystywania jest podstawą do naliczania opłaty [Wiśniewski 2013, s. 78].

Zaletami usługi w modelu SaaS są między innymi: niskie koszty wdrożenia nowego oprogramowania, szybkość wdrożenia, ograniczenie inwestycji w hardware, ograniczone koszty obsługi serwisowej, dostęp do najnowszego oprogramowania, brak konieczności aktualizacji oprogramowania, wreszcie, brak kosztów zakupu licencji na oprogramowanie.

Biorąc pod uwagę istotność danych[4] przechowywanych w repozytorium, sugerowanym modelem wdrożenia projektowanego rozwiązania jest chmura publiczna lub hybrydowa. Public Cloud jest najpopularniejszym i najmniej angażującym klienta rodzajem chmury. Charakteryzuje się tym, że usługa jest dostępna dla każdego zainteresowanego za odpowiednią opłatą abonencką. Przykładem firm oferujących tego typu usługi są między innymi: Google, Microsoft, Amazon oraz z polskiego rynku: Grupa Onet.pl S.A., ATM Systemy Informatyczne S.A. Organizacja korzystająca z chmury publicznej nie musi dbać o zakup hardware'u, nie musi go serwisować i konserwować, oszczędza na zakupie licencji programowych, oszczędza powierzchnię biurową, oszczędza energię elektryczną [Wiśniewski 2013, s. 79].

Alternatywą dla Public Cloud jest chmura hybrydowa (ang. *Hybrid Cloud*), która stanowi dowolne zestawienie rodzajów modeli usług CC[5] oraz modeli wdrożenia CC[6], np.: Public Cloud i Private Cloud, w których część danych przetwarzana jest w chmurze publicznej, a dane niejawne w chmurze prywatnej. Dzięki takiemu rozwiązaniu przedsiębiorstwo ogranicza rozmiar chmury prywatnej, przez co działa zgodnie z prawem i osiąga oszczędności finansowe, które są jednak mniejsze niż w przypadku całkowitego przeniesienia danych do chmury publicznej. Chmura hybrydowa może mieć zastosowanie, jeśli w procesie planowania cywilnego oraz budowy planów ratowniczych i planów zarządzania kryzysowego stosowane są metody i techniki specyficzne, które nie powinny być znane zbyt szerokiemu gronu odbiorców.

Kolejnym zagadnieniem dotyczącym technologii implementacji repozytorium jest realizacja samego repozytorium danych. W tym obszarze istnieje bogaty wachlarz systemów zarządzania bazami danych. Ze względu na zachowanie możliwości równoległego dostępu wielu użytkowników do repozytorium należy zastosować jeden z serwerów baz danych. W tym obszarze do zastosowania są możliwe rozwiązania:

- darmowe: My SQL, Apache Derby, MariaDB, Firebird SQL,
- płatne: MS SQL Server, D2B, Oracle, PostgreSQL.

[4] Dane ogólnodostępne dotyczące znanych metod i technik.

[5] Modele usług CC: Software as a Service, Hardware as a Service, Platform as a Service.

[6] Modele wdrożenia CC: chmura publiczna, chmura prywatna, chmura wspólnotowa, chmura hybrydowa.

Podsumowanie

Wyniki badań przedstawione w artykule stanowią rezultat projektu rozwojowego prowadzonego przez autorów. Opracowana struktura repozytorium dobrych praktyk umożliwia ich charakterystykę w aspekcie procesu planowania cywilnego i zarządzania kryzysowego.

Przedstawiony przykład charakterystyki dwóch metod: metody Preliminary Hazard Analysis oraz „6 kapeluszy", obrazuje sposób posługiwania się repozytorium przez podmioty zaangażowane w publiczne zarządzanie kryzysowe.

Wykonana analiza wymagań niefunkcjonalnych sugeruje technologię implementacji repozytorium dobrych praktyk oraz model udostępniania go użytkownikom.

Bibliografia

Kosieradzka A. (2013), *Metody i techniki pobudzania kreatywności w organizacji i zarządzaniu*, Edu-Libri, Kraków–Warszawa.

Kosieradzka A, Smagowicz J., Wiśniewski M. (2019), *Koncepcja repozytorium dobrych praktyk wykorzystywanych w publicznym zarządzaniu kryzysowym*, „Przegląd Organizacji".

Kosieradzka A., Zawiła-Niedźwiecki J. (2016), *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym*, Edu-Libri, Kraków–Legionowo.

Krupa T., Wiśniewski M. (2015), *Situational Management of Critical Infrastructure Resources United Threat*, „Foundations of Management", vol. 7, annual 2015, ss. 93–104.

Lidwa W. (2015), *Zarządzanie kryzysowe*, AON, Warszawa.

Lis S. (red.) (1999), *Vademecum produktywności*, Placet, Warszawa.

Norma ISO/IEC 31010 – Praktyczne metody oceny ryzyka.

Ostrowska T., Wiśniewski M. (2016), *Wyzwania i dobre praktyki zarządzania bezpieczeństwem infrastruktury krytycznej* [w:] Ćwiklicki M., Jabłoński M., Mazur S. (red.), *Współczesne koncepcje zarządzania publicznego, Fundacja Gospodarki i Administracji Publicznej*, Kraków.

Skomra W. (2015), *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP*, Bel Studio SP. z o.o., Warszawa.

Socha K. (2010), *Inżynieria oprogramowania*, PWN, Warszawa.

Tyburska A. (2009), *Ochrona infrastruktury krytycznej – potrzeby edukacyjne* [w:] T. Białas, M. Grzybowski, J. Tomaszewski, *Zarządzanie bezpieczeństwem w sektorze publicznym i biznesie*, Wyższa Szkoła Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni Gdynia, ss. 83–102

Wiśniewski M., Kunikowski G., Kisilowski M. (2017), *Koncepcja metodycznego gromadzenia wzorców i przykładów dobrych praktyk z zakresu planowania cywilnego oraz budowy planów ratowniczych i planów zarządzania kryzysowego*, Studia i Materiały „Miscellanea Oeconomicae", 4, tom I.

Wiśniewski M. (2013), *Cloud Computing as a Tool for Improving Business Competitiveness*, „Foundations of Management", vol. 5(3), ss. 75–88.

Katarzyna Świerszcz | katarzyna.swierszcz@wat.edu.pl
Wojskowa Akademia Techniczna w Warszawie

Znaczenie energii geotermalnej wobec wyzwań niskiej emisji i ubóstwa ciepła w strategii bezpieczeństwa ekologicznego

Wstęp

Niska emisja jest jednym z najbardziej istotnych, a wręcz priorytetowych tematów poruszanych w polityce i strategii bezpieczeństwa ekologicznego zarówno w Polsce, jak i w pozostałych krajach Unii Europejskiej i świata. Wiąże się to ze wzrostem zagrożeń w obszarze środowiska naturalnego (powietrza, wody, gleby, ekosystemu, zasobów biologicznych, różnorodności ekologicznej i wielu innych). Zagrożenia te są spowodowane niewłaściwym korzystaniem z owych naturalnych dóbr. Ich źródłem jest przede wszystkim niska emisja z gospodarstw domowych, rolnictwa, a także przedsiębiorstw i transportu. Stosowany przez te podmioty system zaopatrzenia w energię cieplną opiera się głównie na paliwach konwencjonalnych, takich jak: węgiel kamienny, węgiel brunatny, ropa naftowa i gaz ziemny. Do paliw najczęściej wykorzystywanych w gospodarstwach domowych należą jednak węgiel i jego pochodne oraz stosowane – ze względu na ubóstwo ciepła – odpady powęglowe, szczególnie tzw. miały, muły czy floty węglowe, zawierające duże ilości popiołów i siarki, które mają niską wartość energetyczną. Stosowanie niskiej jakości źródeł ciepła powoduje stałe przekraczanie dopuszczalnych norm stężenia emisji. Przekroczenia te dotyczą zarówno standardu dobowego, jak i standardu rocznego i występują przede wszystkim w dużych aglomeracjach miejskich. Ważnym problemem w okresie lata jest zbyt wysokie stężenie ozonu troposferycznego, zaś w okresie zimy (tzw. sezonie grzewczym, trwającym od października do marca) – ponadnormatywne stężenie pyłów PM10 (ołów, arsen, kadm, nikiel) i PM2,5 oraz benzopirenu.

Ze względu na stale utrzymujący się na wysokim poziomie stan zanieczyszczenia powietrza w Polsce oraz ze względu na konieczność przestrzegania dopuszczalnych norm emisji zanieczyszczeń, które są ustanowione dyrektywą Parlamentu Europejskiego i Rady, określanej dyrektywą CAFE (Europejski Program Ochrony Klimatu), przed naszym krajem cały czas stoją poważne wyzwania, wśród których priorytetem jest poprawa jakości powietrza. Zadaniu temu służy także zobowiązanie Polski jako członka Wspólnoty Europejskiej do realizacji w ramach pakietu klimatyczno-energetycznego działań określanych mianem 3x20%, które obejmują: redukcję emisji CO_2 o 20% do 2020 r.; zwiększenie efektywności energetycznej o 20% do 2020 r. oraz wzrost zużycia energii z odnawialnych źródeł o 20% do 2020 r. Mając na uwadze powyższe zobowiązania wynikające z przywołanych dokumentów, jak również wielu innych dokumentów unijnych (takich jak np. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu do roku 2020; dyrektywy Parlamentu Europejskiego i Rady Europejskiej odnośnie do stawianych celów w zakresie gospodarki niskoemisyjnej; Plan działania w celu poprawy efektywności energetycznej we Wspólnocie Europejskiej; Europejski Program Zapobiegający Zmianie Klimatu; Zielona Księga Europejskiej Strategii Bezpieczeństwa Energetycznego) i dokumentów krajowych (takich jak np. Założenie Narodowego Programu Rozwoju Gospodarki Niskoemisyjnej; Długookresowa Strategia Rozwoju Kraju – Polska 2030; Strategia Rozwoju Kraju 2020; Strategia Bezpieczeństwa Energetycznego i Środowisko perspektywa 2020 r.; Polityka Energetyczna Polski do 2030 roku; Krajowy plan działań dotyczący efektywności energetycznej; Krajowy plan działania w zakresie energii ze źródeł odnawialnych; Program Operacyjny Infrastruktura i Środowisko 2014–2020; Ustawa o wspieraniu termomodernizacji i remontów; Ustawa o efektywności energetycznej), można uznać, że jednym ze źródeł, które może w pełni sprostać owym wyzwaniom, jest energia geotermalna. Autorka zatem w niniejszym artykule stawia sobie za cel ukazanie, w jaki sposób i w jakim zakresie energia geotermalna może być wyzwaniem dla niskiej emisji, która jest naturalną konsekwencją ubóstwa ciepła gospodarstw domowych, w strategii bezpieczeństwa ekologicznego. Przedstawione propozycje i rozwiązania mogą być w jakimś stopniu pomocą i inspiracją dla innych państw, dla których zjawisko niskiej emisji również jest niepokojącym problemem ekologicznym.

Definicja niskiej emisji i źródła jej powstawania

Termin „niska emisja" można zdefiniować jako emisję szkodliwych pyłów i gazów, które wydobywają się z niskich emitorów, najczęściej kominów znajdujących się na wysokościach do 40 m nad ziemią. Wprowadzane do powietrza na tej wysokości zanieczyszczenia kumulują się w jednym miejscu (szczególnie jeżeli domy znajdują się w kotlinach lub dolinach rzek), w miejscu ich wytwarzania, i mają szkodliwy wpływ na zdrowie człowieka i jego środowisko, zarówno ożywione, jak i nieożywione, w tym infrastrukturę. Wśród substancji tych można wymienić: pyły zawieszone typu: PM10 i PM2,5, dwutlenek siarki (SO_2), tlenki azotu (NO_x), metale ciężkie (m.in. rtęć, kadm, ołów, mangan, chrom), wielopierścieniowe węglowodory aromatyczne (WWA), dioksyny oraz benzo(a)piren [Apte i in. 2017, s. 7009; Dong, Sun, Jiang, Zeng 2018, s. 54].

Pojęcia niskiej emisji nie należy mylić z małą emisją czy też gospodarką niskoemisyjną, która dąży do ograniczania emisji zanieczyszczeń i jest obecnie priorytetowym kierunkiem działań strategii bezpieczeństwa ekologicznego na całym świecie.

Aby uświadomić sobie znaczenie problemu niskiej emisji oraz umieć podjąć właściwe działania zaradcze, trzeba również zastanowić się nad tym, co jest przyczyną niskiej emisji i które źródła jej powstawania wymagają największej uwagi ze względu na szkodliwość działania. Badania pokazują, że niska emisja ma zasadniczo trzy podstawowe źródła. Są nimi: gospodarstwa domowe i rolne, lokalne kotłownie oraz transport [Kumar Verma, Sangle 2015, s. 185]. Każde z tych źródeł zanieczyszczenia ma swoją specyfikę i związany z tym wpływ na środowisko. Dla przykładu, indywidualne gospodarstwa domowe oraz gospodarstwa rolne jedno- i wielorodzinne (których łącznie w Polsce jest ok. 9 mln) w związku z potrzebą zaspokajania swoich podstawowych celów egzystencjalno-bytowych wymagają dużej ilości energii cieplnej, która zużywana jest głównie do ogrzewania pomieszczeń (ok. 69% całej energii), do ogrzewania wody (ok. 15% całej energii) oraz przygotowywania posiłków (ok. 9% całej energii). W tym celu gospodarstwa te wykorzystują podstawowy nośnik energii, jakim są stałe paliwa grzewcze. W ok. 49% są to paliwa słabej lub złej jakości (szczególnie węgiel, drewno, brykiet, biomasa), a nawet odpady, spalane w ilości ok. 2 mln ton w ciągu roku.

Określone zachowania mieszkańców gospodarstw domowych w zakresie wykorzystania paliw grzewczych wynikają z dwóch przyczyn, pomiędzy którymi zachodzi korelacja. Są nimi: wysoka cena energii cieplnej oraz niskie dochody finansowe gospodarstw domowych. Poważnym problemem gospodarstw domowych,

który w istotnym stopniu wpływa na poziom niskiej emisji, jest zły stan techniczny domów, a mówiąc dokładniej, niska efektywność energetyczna budynków, która zależy od: jakości izolacji cieplnej, stopnia szczelności okien, szczelność drzwi balkonowych, szczelność dachu, stanu urządzeń technicznych i instalacji, stopnia sprawności wentylacji itp. Badania przeprowadzone przez autora w latach 2017–2018 z użyciem kamery termowizyjnej pokazują, że duża część budynków (jednorodzinnych, kamienic, bloków) jest całkowicie nieocieplona lub też ocieplona niewystarczająco (ponad 70% z ok. 5 mln domów jednorodzinnych – czyli ok. 3,6 mln), pozostała część w dalszym ciągu wymaga gruntownej termomodernizacji oraz wymiany urządzeń i systemu wytwarzania, regulacji, magazynowania, a także transportu ciepła. Budynki te przynoszą bowiem duże straty energii cieplnej. Innymi słowy, nie służą one racjonalnemu poziomowi zużycia ciepła. Dla przykładu, w energochłonnym budynku jednorodzinnym straty ciepła wynoszą: przez okna – 36,3%, niesprawną wentylację – 30,5%, przez ściany zewnętrzne – 13,3%, przez dach – 13,3%, przez podłogę na gruncie – 4,9%, przez drzwi zewnętrzne – 1,8%. Dotyczy to szczególnie budynków wybudowanych w latach 90. i wcześniej [Świerszcz, Grenda 2018, s. 217]. Nie bez znaczenia jest także powierzchnia mieszkania. Im niższa jest jakość wyżej wymienionych składników efektywności energetycznej budynku, tym wyższe muszą być wydatki – konieczne do zapewnienia komfortu ciepła w okresie zimy lub chłodu w okresie lata. Są one tym wyższe, im większa jest powierzchnia mieszkania. Dla przykładu, mieszkanie większe o 10% zwiększa wydatki na ogrzewanie o 4%. Stopień efektywności energetycznej budynków i związane z nią koszty ponoszone na ciepło uzależniony jest także wyraźnie od wieku budynków. Im budynki są nowsze, tym większa jest ich energooszczędność, a tym samym niższe koszty za ciepło. Dla przykładu, gospodarstwa domowe zamieszkujące budynki powstałe po 2006 r. płacą mniej aż o 17% w stosunku do budynków powstałych wcześniej [Świerszcz 2017a, ss. 175–178; Świerszcz, Grenda, Szczurek, Chen, 2019, ss. 771–779].

Kolejnym czynnikiem związanym z gospodarstwem domowym mającym wpływ na poziom i intensywność niskiej emisji jest nieefektywna, czy wręcz niesprawna, instalacja grzewcza [Świerszcz 2016b, s. 199], a także związane z nią przestarzałe, nieefektywne energetycznie piece, których – jak podaje Instytut Ekonomiki Środowiska – jest ok. 3,5 mln. Korzysta z nich ponad 49% gospodarstw domowych. Przeprowadzone przez autora w latach 2017–2018 badania pokazują, że w gospodarstwach domowych najwięcej jest: kotłów i kominków przeznaczonych na drewno i biomasę – 13,7% (687 tys.); kotłów węglowych o nieustalonych parametrach – 2,4% (120 tys.); kotłów węglowych retortowych mających 10 lat i więcej – 1,5% (75 tys.); kotłów węglowych retortowych poniżej 10 lat – 6,5% (325 tys.); kotłów węglowych zasypowych

mających poniżej 10 lat – 30,1% (1,5 mln) [Świerszcz 2017a, s. 180]. W domach tych są również piece, tzw. kopciuchy (nazywane też „śmieciuchami"), czyli piece górnego spalania, w których można spalać praktycznie wszystko, co jest do nich wrzucane. Piece te charakteryzuje prosta konstrukcja, stosowana praktycznie w niezmienionej wersji (technologii) od ponad 100 lat. „Zaletą" owych pieców jest cena oraz możliwość spalania wszystkich wrzuconych do nich rzeczy, natomiast wadą – ich duża emisyjność i niska efektywność energetyczna, która teoretycznie wynosi 50–60%, jednakże w praktyce jest nawet dwa razy mniejsza [Sadlok 2014, s. 74].

Prezentowany powyżej problem niskiej emisji, dotykający na co dzień mieszkańców gospodarstw domowych, należy łączyć z innym problemem – ubóstwa ciepła gospodarstw domowych [Świerszcz 2017b, ss. 131–138; Poruschi, Ambrey 2018, s. 119]. Dane przedstawione w dotychczasowych rozważaniach wyraźnie pokazują, że zjawisko niskiej emisji, będącej skutkiem ubóstwa ciepła mieszkańców gospodarstw domowych, jest problemem nie tylko środowiskowym, ale także, a może przede wszystkim, problemem o charakterze społecznym, którego konsekwencje niosą wiele zagrożeń, zarówno w ekosystemie, jak i infrastrukturze.

Wpływ niskiej emisji na jakość środowiska i infrastrukturę

Skutki oddziaływania niskiej emisji na środowisko naturalne są odczuwalne w Polsce przez cały rok. Dotyczy to powietrza, wody i gleby, a tym samym wszystkich żywych organizmów, które oddychają i spożywają skażoną wodę oraz żywność. Skutki tego oddziaływania nie są również obojętne dla środowiska materialnego, które tworzy i w którym żyje człowiek.

Najbardziej odczuwalną konsekwencją niskiej emisji jest jej bezpośredni wpływ na kondycję i zdrowie człowieka. Uwidacznia się to najczęściej w chorobach: układu oddechowego (takich jak np. zapalenie błony śluzowej jamy ustnej, zapalenie gardła, przewlekłe zapalenie oskrzeli, nowotwory płuc, przypadki chronicznego kaszlu, niewydolność płuc oraz astma oskrzelowa); zaburzeniach centralnego układu nerwowego (jak np. bezsenność, bóle głowy, złe samopoczucie, zwiększona agresywność); chorobach oczu (jak np. zapalenie spojówek); alergiach; chorobach układu krążenia; osłabieniu płodności, osłabieniu układu immunologicznego, a także nowotworach. Wymienione powyżej czynniki – jak pokazują badania – mają nie tylko wpływ na osłabienie stanu kondycji i zdrowia człowieka, lecz także stanowią główny czynnik śmierci człowieka. Szacuje się, że w Polsce z powodu niskiej emisji umiera 40–45 tys. osób rocznie [Ochoa-Hueso i in. 2017, s. 85].

Niska emisja, osłabiając kondycję zdrowotną człowieka, generuje także koszty ekonomiczne, tzw. koszty zewnętrzne, które ponosi każdy mieszkaniec. Koszty te obejmują w szczególności: wydatki na opiekę zdrowotną, ponoszone bezpośrednio przez osoby chorujące z powodu niskiej emisji, jak również wydatki w ramach systemu opieki zdrowotnej. Należy także zwrócić uwagę na koszty, które wynikają z mniejszej produktywności pracownika, czy nawet jego nieobecności w miejscu pracy z powodu choroby jego lub członków jego rodziny. Szacunkowe koszty ekonomiczne złej jakości powietrza związane z całkowitą emisją pyłu PM2,5 do powietrza wyznaczone dla Krakowa, według metodyki stosowanej w Unii Europejskiej w Programie Czystego Powietrza dla Europy (CAFE-CBA), wynoszą 740 mln zł rocznie [Małochleb 2017, s. 43; Rao i in. 2017, ss. 348–355].

Skutki niskiej emisji widoczne są również w jej oddziaływaniu na stan i jakość dóbr materialnych. Uwidacznia się to w niszczeniu czy wręcz degradacji zabytków (dziedzictwa kulturowego) i fasad budynków zarówno mieszkalnych, jak i użyteczności publicznej. Kruszące się i odpadające tynki czy też pokryte ciemnym nalotem budynki, zmieniające się zabarwienia ścian i dachów to jeden z wielu przykładów działania siarki i innych związków chemicznych, które w sposób istotny zmniejszają atrakcyjność wizualną i inwestycyjną nie tylko budynków, ale także całego miasta. Znacząco obniżają tym samym również jego walory turystyczne. Niska emisja, oddziałując negatywnie na stan i jakość budynków, także i w tym przypadku zwiększa koszty ekonomiczne związane z koniecznością podejmowania częstszych i bardziej rozległych renowacji. Ich koszty liczone są w milionach złotych rocznie. Innym skutkiem niskiej emisji jest korozja metali oraz zwiększone zużycie maszyn i urządzeń. Obecność niskiej emisji (połączonej siarki i tlenu w różnych związkach oraz dwutlenku węgla) znacząco przyspiesza naturalny proces korozji metali, co w konsekwencji wpływa na zwiększone zużycie maszyn i różnego rodzaju urządzeń, z których codziennie korzysta człowiek. Tym samym powoduje to skrócenie ich żywotności. Wyraźnie odczuwalnymi skutkami niskiej emisji są także: przyspieszone niszczenie skóry, papieru i odzieży, a także wydłużony czas wysychania farb i lakierów [Sadlok 2014, s. 51].

Energia geotermalna jako wyzwanie wobec niskiej emisji i ubóstwa ciepła

W działaniu na rzecz skutecznego zmniejszania niskiej emisji i ubóstwa ciepła gospodarstw domowych zarówno w miastach, jak i na wsiach ważną rolę obecnie zdaje się spełniać energia geotermalna. Przemawia za nią wiele argumentów, wśród których

szczególnie istotne są dwa: znaczne ograniczenie ilości emisji zanieczyszczeń (zwłaszcza w sezonie zimowym) oraz stosunkowo niskie ceny energii cieplnej [Świerszcz, Ćwik 2017, s. 144; Świerszcz 2019, s. 83; Loppi, Nascimbene 2010, ss. 2635–2639]. Przykładem szerokiego wykorzystania energii geotermalnej jest miasto Zakopane. Dzięki zastosowanym sieciom ciepłowniczym podłączonym do ciepłowni geotermalnej „PEC Geotermia Podhalańska S.A.", dostarczającej ciepło całemu miastu i okolicznym mieszkańcom, dotychczasowy poziom emisji zanieczyszczeń uległ wyraźnej redukcji na całym Podhalu. Potwierdzają to poniższe dane: CO_2 – redukcja aż do 39,6 tys. ton/rok; SO_2 – emisja jedynie 12 µg/m^3/rok; PM10 – emisja jedynie 32 µg/m^3/rok. Dzięki temu w latach 1999–2016 ograniczono ilość wykorzystania węgla – do 243,3 tys. ton oraz emisję CO_2 – do 488 tys. ton. Dane te zostały udostępnione przez firmę „PEC Geotermia Podhalańska S.A.". Ciepłownia geotermalna dysponuje obecnie siecią ciepłowniczą o długości ponad 100 km, przez którą dostarczane jest ciepło do okolicznych wsi i mieszkańców Zakopanego. Integralną część systemu ciepłowniczego – jak mówi Prezes Zarządu Geotermii Podhalańskiej Wojciech Ignacok – stanowi znajdująca się w Zakopanym ciepłownia o mocy 42 MW. Kotłownia pełni rolę źródła szczytowego, które współpracuje z układem ciepłowni geotermalnej. Ciepłownia ta pozyskuje 70,7 MWt energii geotermalnej (całkowita moc – 80,5 MWt). U każdego odbiorcy ciepła geotermalnego jest zainstalowany indywidualny węzeł grzewczy, który jest dostosowany do potrzeb odbiorcy, obejmujący: centralne ogrzewanie (c.o.) i przygotowanie ciepłej wody użytkowej (c.w.u.). W sieci występują trzy rodzaje indywidualnych węzłów z wymiennikami o mocach: 15 kW c.o./33 c.w.u.; 25 kW c.o./43 kWc.w.u. i 33 kW c.o./50 kW c.w.u. W zależności od wybranej grupy taryfowej ustalone są określone taryfy cen i stawki opłat. Grupa taryfowa (M1, M2, M4) – cena ciepła to 19,01 zł/GJ, zaś cena nośnika ciepła to 17,43 zł/m^3; grupa taryfowa (G) – cena ciepła to 16,52, zaś cena nośnika ciepła to 3,35 zł/m^3 [Ignacok 2017, ss. 13–15; Decyzja 2018, s. 48].

W ostatnich latach według danych „PEC Geotermia Podhalańska S.A." poziom sprzedaży energii cieplnej z geotermii kształtował się następująco: w 2010 r. – 376 195 GJ; w 2011 r. – 352 842 GJ; w 2012 r. – 383 738 GJ; w 2013 r. – 393 117 GJ; w 2014 r. – 361 634 GJ; w 2015 r. – 398 522 GJ; w 2016 r. – 421 130 GJ. Dane te wyraźnie pokazują, że sprzedaż energii cieplnej pozyskiwanej z energii geotermalnej stale rośnie, co wskazuje na ciągłe zainteresowanie tym rodzajem ciepła wśród jej odbiorców. Ze względu na wymienione walory ciepło geotermalne jest szczególnym dobrem w strukturze produkcji ciepła na tle pozostałych źródeł pozyskiwania ciepła. Dla przykładu, pozyskiwanie ciepła w 2015 r. było na poziomie: z energii geotermalnej – 90%; z gazu – 10%; z oleju – 0%. Natomiast pozyskiwanie ciepła w 2016 r. kształtowało się na poziomie: z energii geotermalnej – 91%; z gazu – 9%; z oleju – 0% [Ignacok 2017, s. 17].

Klientami ciepła geotermalnego, jak mówi Prezes Zarządu Geotermii Podhalańskiej, są przede wszystkim mieszkańcy, instytucje i przedsiębiorstwa, w łącznej liczbie 1473. W tym z Zakopanego – 1135 odbiorców, czyli 77,1%; Białego Dunajca – 164 odbiorców, czyli 11,1%; Szaflar – 146 odbiorców, czyli 9,9% i Poronina – 28 odbiorców, czyli 1,9%. Geotermia Podhalańska dostarcza energię cieplną do 1473 obiektów, z czego najwięcej stanowią budynki jednorodzinne – w liczbie 834, czyli 56,6%, i budynki pozostałe – w liczbie 639, czyli 43,38%. Na te ostatnie składają się: budynki wielorodzinne – w liczbie 278, czyli 18,9%; budynki usługowo-handlowe – w liczbie 122, czyli 8,3%; hotele, pensjonaty, domy wczasowe – w liczbie 103, czyli 7,0%; szkoły, przedszkola, sale gimnastyczne – w liczbie 35, czyli 2,4% oraz inne obiekty – w liczbie 101, czyli 6,9%. Najwięcej ciepła geotermalnego PEC Geotermia Podhalańska sprzedaje do budynków wielorodzinnych, usługowych, użyteczności publicznej, hoteli itp. – 354 089 GJ, czyli 84,08%, natomiast pozostała część energii jest sprzedawana do budynków jednorodzinnych – w ilości 67 041GJ, czyli 15,92% [Ignacok 2017, s. 15; Świerszcz 2018, ss. 329–333].

Ze względu na duże zainteresowanie energią ciepła geotermalnego wśród mieszkańców Zakopanego i jego okolic w 2016 r. po raz pierwszy w historii PEC GT dokonała obniżki cen owego ciepła. Jednakże jeszcze rok wcześniej, tj. w 2015 r., ciepło to – według zestawienia przygotowanego przez Urząd Regulacji Energetycznej (URE) – było droższe od ciepła wytwarzanego z węgla brunatnego i kosztowało odpowiednio: 32,38 zł za GJ i 26,08 zł za GJ. Cena ta jednak była niższa niż cena energii cieplnej powstałej z miału węgla kamiennego (która wynosiła 37 zł) oraz wytworzonej przy użyciu gazu (która wynosiła ponad 50 zł za GJ). W tym czasie w 2016 r. Zakład Geotermii Podhalańskiej wytworzył ponad 90% energii cieplnej, pozostała część ciepła pochodziła z gazu (niecałe 9%) i oleju (ułamek 1%). Jak pokazują badania gospodarstw domowych, cena ogrzania domu o powierzchni ok. 150m^2 wynosi ok. 400 zł miesięcznie. Analiza cen ciepła pozyskanego z innych źródeł, takich jak: węgiel brunatny, węgiel kamienny, paliwa pozostałe, olej opałowy, gaz ziemny – wyraźnie pokazuje znaczącą różnicę na korzyść ciepła uzyskiwanego z zasobów energii geotermalnej [Ignacok 2017, s. 17; Świerszcz 2016b, s. 203; Świerszcz, Szczurek, Mitkow, Zalewski, Ćwik 2019, s. 2173].

Korzystne wyniki osiągane w cenie ciepła rodzą stałe zainteresowanie potencjalnych klientów zarówno gospodarstw domowych, instytucji, jak i przedsiębiorców, szczególnie zajmujących się hotelarstwem. Ich obecna liczba wynosi ok. 77% społeczności Zakopanego i okolic. Zainteresowanie ciepłem geotermalnym widoczne jest także w pobliskich miejscowościach, czego przykładem jest Nowy Targ, który, chcąc ogrzewać miasto bardziej ekonomicznie, podjął decyzję o przyłączeniu się do sieci ciepłowniczej Geotermii Podhalańskiej.

Zakończenie

Dbanie o jakość powietrza atmosferycznego jako jednego z elementów środowiska naturalnego należy do priorytetowych zadań strategii i polityki bezpieczeństwa ekologicznego Polski. Pomimo stopniowej poprawy jakości powietrza w naszym kraju problem niskiej emisji jako naturalnej konsekwencji ubóstwa ciepła wielu gospodarstw domowych jest nadal aktualny. Stale zwiększające się zapotrzebowanie na energię cieplną wśród mieszkańców gospodarstw domowych, które wynika z potrzeby podnoszenia jakości życia społecznego, w tym zaspokajania potrzeb socjalno-bytowych gospodarstw domowych, jest naturalną konsekwencją i ceną, jaką płacimi za wzrost gospodarczy i postęp cywilizacyjny. Z drugiej strony, utrzymujące się zjawisko ubóstwa ciepła powoduje, że głównym źródłem owego ciepła jest paliwo niskiej jakości, a nierzadko wręcz odpady. Istotnym problemem sprzyjającym niskiej emisji są także lokalne nieefektywne energetycznie kotłownie węglowe i domowe piece grzewcze, w których spalanie węgla dokonuje się w nieefektywny sposób, najczęściej tanim węglem o niskich parametrach grzewczych.

Alternatywnym rozwiązaniem, umożliwiającym wyjście naprzeciw wyzwaniom dotyczącym ograniczenia niskiej emisji substancji szkodliwych do atmosfery w wyniku doświadczanego ubóstwa ciepła gospodarstw domowych, wydają się być energia geotermalna oraz związane z nią geotermalne ciepłownie (sieci ciepłownicze), które wpisują się w realizację szeroko rozumianej gospodarki niskoemisyjnej, stanowiącej priorytetowy cel polityki i strategii bezpieczeństwa ekologicznego naszego państwa. Potwierdzają to liczne przykłady polskich miast, takich jak: Pyrzyce, Uniejów, Stargard, Mszczonów, Zakopane i okoliczne miejscowości, Konin i wiele innych. Zastosowana tam energia geotermalna w bardzo odczuwalnym stopniu nie tylko obniża cenę energii ciepła, lecz także poprawia jakość powietrza. Wynika to z tego, że energia geotermalna jest ekologicznym źródłem energii, ponadto cena energii pozyskiwanej z zasobów geotermalnych, w przeciwieństwie do konwencjonalnych źródeł energii, jest stosunkowo niska. Wykorzystanie energii geotermalnej niesie wiele korzyści zdrowotnych i społecznych, takich jak: podniesienie jakości życia społeczeństwa, stanu zdrowia ludności, poprawa środowiska naturalnego, zwiększenie atrakcyjności inwestycyjnych danego obszaru, poprawa jego walorów turystycznych i klimatycznych i wreszcie ograniczenie kosztów leczenia chorób oraz renowacji budynków i zabytków.

Mając powyższe na uwadze, należy zauważyć, że ważnym zadaniem staje się dzisiaj uświadamianie, iż inwestycja w odnawialne źródła energii, do których między innymi należy energia geotermalna, stanowi inwestycję przyszłościową.

Inwestycję, która umożliwia zrównoważony rozwój szeroko rozumianej konkurencyjnej gospodarki niskoemisyjnej, a także wprowadzenie efektywnych i inteligentnych geotermalnych sieci energetycznych ciepła.

Bibliografia

Apte J.S. i in. (2017), *High-Resolution Air Pollution Mapping with Google Street View Cars: Exploiting Big Data*, „Environ Sci Technol", vol. 51.

Decyzja nr OKR-4210-14(20)/2017/2018/401/X/UJN Prezesa Urzędu Regulacji Energetyki z dnia 29 stycznia 2018 roku w sprawie zatwierdzenia taryfy dla ciepła Przedsiębiorstwa Energetyki Cieplnej „Geotermia Podhalańska" S.A. z siedzibą w Bańskiej Niżnej, poz. 820.

Dong K., Sun R., Jiang H, Zeng X. (2018), *CO2 emissions, economic growth, and the environmental Kuznets curve in China: What roles can nuclear energy and renewable energy play?*, „Journal of Cleaner Production", vol. 196.

Ignacok W. (2017), *Doświadczenia z podłączenia domów jednorodzinnych do sieci ciepłowniczych PEC Geotermia Podhalańska S.A.*, Geotermia Podhalańska, Kraków.

Loppi S., Nascimbene J. (2010), *Monitoring H2S air pollution caused by the industrial exploitation of geothermal energy: The pitfall of using lichens as bioindicators*, „Environmental Pollution", vol. 158.

Kumar Verma Bhupendra K., Sangle S. (2015), *What drives successful implementation of pollution prevention and cleaner technology strategy? The role of innovative capability*, „Environmental Science and Technology", vol. 155.

Małochleb M. (2017), *Niska emisja – przewodnik*, Fundacja Centrum Edukacji Obywatelskiej, Warszawa.

Ochoa-Hueso R. i in. (2017), *Ecological impacts of atmospheric pollution and interactions with climate change in terrestrial ecosystems of the Mediterranean Basin: Current research and future directions*, „Environmental Pollution", vol. 227.

Poruschi L., Ambrey Ch.L. (2018), *Densification, what does it mean for fuel poverty and energy justice? An empirical analysis*, ,,Energy Policy", vol. 117.

Rao S. i in. (2017), *Future air pollution in the Shared Socio-economic Pathways*, ,,Global Environ Chang", vol. 42.

Sadlok R. (2014), *Przeciwdziałanie niskiej emisji na terenach zwartej zabudowy mieszkalnej*, Bochnia: Stowarzyszenie na rzecz efektywności energetycznej i rozwoju odnawialnych źródeł energii ,,HELIOS", Bochnia.

Świerszcz K., Grenda B., *Geothermal Energy as an Alternative Source and a Countermeasure Against Low Emission in the Ecological Security Strategy* [w:] *2018 Joint International Conference on Energy, Ecology and Environment (ICEEE 2018) and International Conference on Electric and Intelligent Vehicles (ICEIV 2018)*, ss. 1–6.

Świerszcz K., Grenda B. (2018), *Poziom ubóstwa energetycznego w wybranych regionach kraju jako miernik poziomu bezpieczeństwa energetycznego w wymiarze społecznym*, ,,Przedsiębiorczość i Zarządzanie", t. XIX, z. 2, cz. 3.

Świerszcz K. (2016a), *Bezpieczeństwo energetyczne Polski – wybrane aspekty obronne* [w:] *Energetyka – szanse, wyzwania i zagrożenia. Logistyka – ekonomia – prawo – polityka – bezpieczeństwo – obronność – technika*, Fundacja na rzecz Czystej Energetyki, Poznań.

Świerszcz K. (2017), *The Impact of Energy Poverty on the Level of Social Security* [w:] 2017 *4th International Conference on Management Science and Management Innovation*, Hui-Ming Wee, ATLANTIS PRESS, Suzhou, China. DOI: https://doi.org/10.2991/msmi-17.2017.39.

Świerszcz K. (2019), *Postrzeganie bezpieczeństwa energetycznego w kontekście przeciwdziałania ubóstwu energetycznemu społeczności lokalnej z wykorzystaniem zasobów geotermalnych na terenie Gminy Wiśniowa*, WAT, Warszawa.

Świerszcz K. (2016b), *Obrona bezpieczeństwa energetycznego Polski w aspekcie geotermalnych dóbr narodowych*, ,,Przedsiębiorczość i Zarządzanie", t. XVII, z. 5, cz. I.

Świerszcz K. (2017b), *Ubóstwo energetyczne jako wskaźnik poziomu bezpieczeństwa energetycznego gospodarstw domowych*, ,,Przegląd Nauk o Obronności", nr 3.

Świerszcz K. (2018), *Wpływ energii geotermalnej w przeciwdziałaniu zanieczyszczeniu środowiska naturalnego* [w:] Z. Trejnis, L. Kościelecki (red.), *Wyzwania i zagrożenia bezpieczeństwa i obronności RP w XXI wieku w wymiarze społecznym i technologiczno-środowiskowym*, ASPRA-JR, Warszawa.

Świerszcz K., Ćwik B. (2017), *Geothermal energy as a Part of Non-military Defence Strategy in the Contex of the Prevention of Energy Poverty of Local Communities*, ,,Przedsiębiorczość i Zarządzanie'', t. XVIII, z. 5, cz. I.

Świerszcz K., Grenda B., Szczurek T., Chen B. (2019), *The Importance of Geothermal Energy in Energy Security: Towards Counteracting Energy Poverty of Households* [w:] *The 33rd International Business Information Management Association Conference (IBIMA)*, K.S. Soliman (red.), Granada, Spain 10-11 April 2019, p. 771-781 (ISBN: 978-0-9998551-2-6).

Świerszcz K., Szczurek T., Mitkow S., Zalewski J., Ćwik B. (2019), *Knowledge of the problem of fuel poverty among local government authorities – in the aspect of local energy security*, Journal of Eastern Europe Research in Business and Economics (JEERBE), IBIMA Publishing, USA 2019. Journal website: www.ibimapublishing.com, http://ibimapublishing.com/articles/JEERBE/2019/780276/, vol. 2019, article ID 780276, 12 pages, ISSN: 2169-0367; DOI: 10.5171/2019.780276.

Włodarczyk E. (2018), *Edukacja dla bezpieczeństwa* [w:] O. Wasiuta, R. Klepka, R. Kopeć (red.), *Vademecum bezpieczeństwa*, Libron, Kraków.

Michał Piekarski | michal.piekarski@uwr.edu.pl
Uniwersytet Wrocławski, Instytut Studiów Międzynarodowych

Zamachy z użyciem urządzeń wybuchowych w możliwych scenariuszach wojny hybrydowej w Polsce

Wstęp

Problematyka formy konfliktów nazywanych zbiorczo wojną hybrydową stała się istotnym elementem narracji dotyczącej bezpieczeństwa państwa w okresie po kryzysie ukraińskim (po roku 2014) i w sposób oczywisty dotyczy także bezpieczeństwa Polski. Pojawia się więc oczywiste pytanie, które brzmi jakie są możliwe scenariusze wojny hybrydowej na terytorium naszego kraju. Pytanie to nadało ogólną formę artykułowi. Z uwagi na szeroki zakres problemu, w niniejszym tekście ograniczono się jedynie do takich scenariuszy, w których istotną rolę odegrać mogą działania mające formę zamachów terrorystycznych z użyciem urządzeń wybuchowych. Analiza zagadnień związanych z innymi możliwymi metodami działania (sytuacje zakładnicze, zamachy z użyciem broni palnej, ataki w cyberprzestrzeni) wymaga dalszych badań i analiz.

Wojna hybrydowa – problemy definicyjne

Termin wojna hybrydowa jest, jak już wspomniano wyżej, szeroko używany od pięciu lat, choć część badaczy zwraca uwagę na fakt, że samo pojęcie było używane wcześniej do opisania konfliktów zbrojnych, których specyfika i sposób użycia siły, nie tylko siły zbrojnej, wykraczał poza ramy konwencjonalnego konfliktu międzypaństwowego. Spory w środowisku naukowym budzą także inne kwestie, związane z samą genezą tego pojęcia. Zostały one szeroko omówione w numerze specjalnym

czasopisma „Przegląd Bezpieczeństwa Wewnętrznego", więc nie będą one szerzej omawiane w niniejszym tekście [Przegląd Bezpieczeństwa Wewnętrznego 2015]

Warto natomiast zauważyć, mając na uwadze nakreślone we wstępie pytanie badawcze, że amerykański badacz F.G. Hoffman już w roku 2009 zdefiniował zagrożenia hybrydowe jako sytuację, gdy „przeciwnik w sposób jednoczesny i adaptując się do pojawiających się w przestrzeni walki warunków stosuje zintegrowaną/połączoną mieszankę broni konwencjonalnej, taktyki nieregularnej, działań terrorystycznych i przestępczych, celem osiągnięcia własnych celów politycznych" [Hoffman 2009]. Z kolei analitycy działającego pod auspicjami NATO programu Multinational Capability Development Campaign w raporcie na temat wojny hybrydowej proponują następującą definicję: „zsynchronizowane użycie wielu instrumentów siły dopasowane do określonych podatności w całym spektrum funkcji społeczeństwa dla osiągnięcia efektu synergii" [Cullen, Reichborn-Kjennerud 2017]

W wymiarze praktycznym środki jakie używane są podczas działań hybrydowych znamionują się więc użyciem w sposób jednoczesny i wzajemnie powiązany rożnych elementów potencjału państwa, od działań informacyjnych, poprzez ekonomiczne, społeczne, polityczne i wreszcie wojskowe. Oznacza to, że zachodzi wówczas sytuacja odmienna niż podczas konwencjonalnego konfliktu zbrojnego, gdy działania konwencjonalne (otwarte starcia sił regularnych) były nadrzędne wobec innych, także niezbrojnych działań. Przykładowo podczas II wojny światowej wykorzystywano, czasem na dużą skalę, działania partyzanckie, ale ich strategicznym celem było stworzenie dogodnej sytuacji na konwencjonalnym polu walki, na przykład poprzez dywersję na liniach kolejowych, co utrudniało przewóz wojsk i zaopatrzenia na front, czy też poprzez sabotaż w fabrykach zbrojeniowych, co obniżało zdolność bojową jednostek, do których trafiały niepełnowartościowe egzemplarze sprzętu wojskowego.

Mając na uwadze kwestię zagrożeń terrorystycznych, należy także zauważyć, że w przypadku działań hybrydowych, lokują się one w szarej strefie pomiędzy czasem pokoju a konwencjonalnej wojny i są trudne do jednoznacznego określenia z uwagi na czynniki polityczne, strategiczne, prawne oraz zakres stosowanej siły zbrojnej [Barno, Benshel 2015]. Mieści się w tym użycie przez agresora wojsk specjalnych, sił nieregularnych oraz zorganizowanych grup przestępczych, w sposób trudny do jednoznacznej identyfikacji przez światową opinię publiczną, co może utrudnić udzielenie zaatakowanemu państwu pomocy sojuszniczej lub reakcję organizacji międzynarodowych, gdyż działania agresora będą upozorowane na aktywność podmiotów niepaństwowych, stwarzającą wrażenie że zaistniały kryzys jest jedynie wewnętrzną sprawą zaatakowanego państwa.

Należy mieć przy tym na uwadze, że hybrydowość konfliktu nie polega tylko na wykorzystaniu wszystkich słabości przeciwnika i równoczesnym oddziaływaniu wojskowym (skrytym lub, w późniejszej fazie konfliktu, jawnym), dyplomatycznym, informacyjnym i gospodarczym. Aktywność agresora ma miejsce zarówno w środowisku lądowym, morskim, przestrzeni powietrznej, cyberprzestrzeni, jak i w środowisku informacyjnym. Stwarza to dodatkowe problemy związane z szybką identyfikacją faktycznych sprawców działań i podjęciem adekwatnej reakcji [Chambers 2016]. Ogranicza to także inne czynniki ryzyka związane z podjęciem otwartych działań zbrojnych, w tym redukuje czynnik przewagi technicznej – co jest szczególnie istotne jeśli rozważa się konflikt hybrydowy na kontynencie europejskim. Pozwala to także agresorowi ograniczyć koszty i straty, jakie poniesione byłyby na skutek przy użycia sił konwencjonalnych.

W sposób oczywisty wyznacza to kontekst podejmowania aktywności terrorystycznej w tego rodzaju konflikcie, w tym z użyciem szeroko pojętych urządzeń wybuchowych. Działalność terrorystyczną w tym kontekście należy więc rozpatrywać mając na uwadze poniższe warunki brzegowe.

Po pierwsze, nie są one celem samym w sobie. Są one częścią długofalowej i wieloaspektowej strategii, zatem pod względem atakowanych celów i sposobu działania sprawców muszą być jej podporządkowane.

Po drugie, jest to element działań prowadzonych przez państwo, w ramach jego polityki. Oznacza to, że mają one na celu realizację polityki jednego państwa wobec drugiego. W związku z tym atak będzie miał na celu wywarcie wpływu na funkcjonowanie całego aparatu państwowego i społeczeństwa, jak również na skomplikowanie sytuacji międzynarodowej.

Zamachy terrorystyczne w wojnie hybrydowej

Powyżej opisane czynniki oznaczają, że mogą mieć miejsce dwa rodzaje zamachów terrorystycznych. Mogą to być zamachy osłabiające państwo, których celem będzie zakłócenie funkcjonowania państwa jako systemu (lub jego podsystemów) lub zamachy o charakterze prowokacji politycznej, mające na celu skomplikowanie sytuacji wewnętrznej, poprzez nasilenie istniejących konfliktów politycznych i społecznych, co doprowadzić może do wywołania kryzysu politycznego o skali uniemożliwiającej podjęcie przez rząd skutecznej reakcji na zagrożenie zewnętrzne.

Determinuje to cele, które będą atakowane. W pierwszym przypadku będą to obiekty ważne dla funkcjonowania państwa, a więc obiekty infrastruktury

krytycznej, w tym węzły komunikacyjne i instalacje energetyczne – elektrownie, rafinerie, składy paliw, linie przesyłowe, infrastruktura teleinformatyczna, strategicznie ważne zakłady przemysłowe[1] oraz obiekty wojskowe i policyjne. W tym ostatnim przypadku celem ataku jest wykazanie nieudolności sił zbrojnych i służb bezpieczeństwa państwa jako niezdolnych ochronić samych siebie – co może zostać łatwo zdyskontowane propagandowo.

W drugim przypadku cele ataków będą miały charakter symboliczny. Chodzi tu zarówno o osoby, jak i o obiekty i wydarzenia (np. demonstracje i imprezy masowe), a intencją sprawców będzie wywołanie silnych reakcji emocjonalnych – strachu oraz oburzenia – przekładających się na zachowania polityczne całych grup społecznych. Działania te mogą być podejmowane w sposób sugerujący, że sprawcami będą członkowie faktycznie istniejących miejscowych ugrupowań politycznych, a może się okazać, że organizacje takie zostaną specjalnie stworzone na potrzeby takiej działalności. Współcześnie wystarczy do tego po prostu założenie kont w mediach społecznościowych w celu zaistnienia, choćby szczątkowego, w przestrzeni medialne.

Można ocenić, że w tym przypadku cel i czas ataku wraz z towarzyszącą mu aktywnością polityczną i medialną dobrane będą w taki sposób, aby wspomniane reakcje wywołały wymierny efekt polityczny, na przykład przekładający się na wynik wyborów lub wystąpienie masowych protestów społecznych. W szczególności kluczowe jest doprowadzenie do sytuacji, w której rząd atakowanego państwa nie byłby politycznie zdolny do wprowadzenia stanu wyjątkowego lub wojennego i sięgnięcia po związane z tym narzędzia.

W obydwu przypadkach, w celu zachowania zdolności do wiarygodnego zaprzeczenia przez państwo stojące za tymi zamachami, możliwe jest przeprowadzenie ataków za pomocą osób, które nie będą jednoznacznie identyfikowane z tym państwem. Najbardziej wygodną grupą sprawców w tym kontekście są oczywiście zwerbowani, z pobudek finansowych lub ideologicznych, obywatele państwa będącego celem, co pozwala nie tylko wykorzystać w pełni ich znajomość lokalnych warunków, ale również w razie ujawnienia tożsamości sprawców daje szansę przedstawienia ich działań jako aktywności niezależnego od obcych wpływów i inspiracji ugrupowania politycznego. Przykładem takiej sytuacji były działania prowadzone przez rząd USA wobec Kuby we wczesnych latach sześćdziesiątych dwudziestego

[1] Nie chodzi tu tylko o zakłady zbrojeniowe czy inne ważne zakłady w czasie konwencjonalnej wojny, ale także o takie przedsiębiorstwa (w tym oddziały korporacji ponadnarodowych), które mają znaczenie dla długoterminowej stabilności ekonomicznej państwa.

wieku, z wykorzystaniem emigrantów politycznych. Możliwe jest także wykorzystanie w tej roli obywateli państwa trzeciego, także działających z pobudek ideologicznych lub materialnych, co także spełnia warunek wiarygodnego zaprzeczenia. Jest to opcja szczególnie wygodna jeśli atakowane państwo jest podatne na zakłócenie relacji z państwem trzecim, na przykład na tle mniejszości etnicznych. Możliwe jest wreszcie wykorzystanie obywateli państwa własnego pozyskanych specjalnie w tym celu – przykładem mogą być próby zabicia Fidela Castro przez CIA z wykorzystaniem członków zorganizowanych grup przestępczych (mafii włoskiej). Może także mieć miejsce wykorzystanie do zamachu żołnierzy wojsk specjalnych lub funkcjonariuszy służb wywiadowczych, oczywiście ukrywających swoją prawdziwą tożsamość, a ataki byłyby przeprowadzone w sposób sugerujący, że sprawcami są inni aktorzy (ludność miejscowa lub z państwa trzeciego). Opcja ta jest politycznie kłopotliwa w razie schwytania takich osób, gdyż oznaczałoby, że państwo wysyłające takich funkcjonariuszy lub żołnierzy nie mogłoby otwarcie potwierdzić ich tożsamości, a wręcz musiałoby przedstawić ich jako osoby, które działały sprzecznie z jego wolą lub w ogóle zaprzeczyć, że są to osoby mające jakiekolwiek powiązania ze służbami specjalnymi lub wojskiem [Kubiak, Makowski 1998]. Te czynniki oznaczają, że najbardziej prawdopodobne jest wykorzystanie czynnych lub byłych żołnierzy lub funkcjonariuszy w charakterze doradców lub instruktorów. Znane są przypadki zdarzeń, gdzie prawdopodobnie wykonawcami byli czynni lub (oficjalnie) byli oficerowie służb specjalnych, ale miały one raczej charakter skrytobójstw (zwłaszcza z wykorzystaniem trucizn) niż zamachów terrorystycznych, co ograniczało ryzyko szybkiej identyfikacji i ujęcia bezpośrednich wykonawców.

Jednocześnie nawet pośredni udział sił i służb specjalnych oznacza, że zagrożenie terrorystyczne w wojnie hybrydowej odbiega od trendów obserwowanych w ciągu ostatnich lat w działalności terrorystycznej w Europie. Zamiast agitacji skutkującej radykalizacją i podjęciem próby dokonania zamachu przez sprawców dysponujących ograniczonymi zasobami, przy użyciu łatwo dostępnych środków lub przystąpienia do aktywnej poza Europą organizacji terrorystycznej, możliwe jest podjęcie przez służby wywiadowcze penetracji licznych środowisk, wytypowanie podatnych na różne rodzaje zachęt osób i prowadzenie wobec nich aktywnej działalności werbunkowej. Wytypowane i zwerbowane osoby mogą zostać poddane procesowi szkolenia, prowadzonego w warunkach konspiracji obejmującego taktyki, techniki i procedury działań typowe dla wojsk specjalnych, jak również, jeśli zajdzie taka potrzeba, zostać przeszkolone w obsłudze specjalistycznego wyposażenia i uzbrojenia. Państwo kierujące takimi działaniami może zapewnić, oprócz owego wyposażenia i uzbrojenia, dostęp do relatywnie dużych

środków finansowych, jak również informacji rozpoznawczych. Możliwe jest także wykorzystanie wcześniej zwerbowanych agentów uplasowanych w atakowanych obiektach, w celu ułatwienia do nich dostępu wykonawcom zamachu.

Ponadto, w przypadku osób dokonujących ataków, istotną zachętą może być obietnica uzyskania schronienia na terenie państwa inspirującego atak. Taka sytuacja przypomina oczywiście znaną z czasów zimnej wojny kooperację państw bloku wschodniego, zwłaszcza ZSRR, NRD i Czechosłowacji z aktywnymi na Zachodzie organizacjami terrorystycznymi, głównie skrajnie lewicowymi. Nie chodzi tu tylko o sam schemat powiązań. Mając na uwadze obecną sytuację geopolityczną, to właśnie Rosja jest najbardziej prawdopodobnym aktorem mogącym zastosować narzędzia wojny hybrydowej w Europie Środkowej i Wschodniej, zwłaszcza w kontekście doświadczeń z kryzysu krymskiego i walk na wschodzie Ukrainy.

Polska jako cel ataków hybrydowych

Takie rozważania w kontekście Polski oznaczają konieczność uwzględnienia kilku warunków brzegowych wynikających z sytuacji wewnętrznej i uwarunkowań międzynarodowych.

Należy przede wszystkim pamiętać, że Polska sama w sobie nie jest państwem posiadającym istotne dla Rosji zasoby naturalne, nie ma także w Polsce – inaczej niż w państwach bałtyckich czy na Ukrainie - dużej mniejszości rosyjskojęzycznej. W roku 2011 tylko trzynaście tysięcy osób zadeklarowało identyfikację z narodowością rosyjską [*Ludność. Stan i struktura demograficzno-społeczna. Narodowy Spis Powszechny Ludności i Mieszkań* 2011]. Bardziej prawdopodobne jest wykorzystanie siły w celu wymuszenia na Polsce określonego, pożądanego przez Rosję zachowania, tak aby uniemożliwić lub utrudnić reakcję NATO na sytuacje kryzysowe, które mogą zaistnieć na wschód od Polski, w obszarze byłego ZSRR, co obejmuje zwłaszcza republiki bałtyckie będące państwami członkowskimi NATO i Unii Europejskiej. Oprócz samego przejęcia lub umocnienia kontroli nad tymi obszarami, co ma swój wymiar geopolityczny (szeroki dostęp do Bałtyku, obecnie bardzo ograniczony dla Rosji), pozwoliłoby to wykazać nieefektywność zachodnich struktur bezpieczeństwa i obrony. W tym kontekście Polska jest państwem, przez które

mogą przemieszczać się sojusznicze siły wzmocnienia[2] i na którego terytorium siły te mogą bazować. Należy także mieć na uwadze własny potencjał militarny Polski, mogący być w niektórych aspektach dla Rosjan kłopotliwy, zwłaszcza w perspektywie jego możliwej modernizacji. Chodzi tu głównie o systemy rakietowe eksploatowane w Marynarce Wojennej (pociski NSM i RBS-15) potencjalnie mogące blokować aktywność floty rosyjskiej na Bałtyku. Także czterdzieści osiem samolotów F-16C/D może mieć istotne znaczenie w konflikcie konwencjonalnym, zwłaszcza jako element sił koalicyjnych.

Celem rosyjskich działań hybrydowych byłoby więc utrudnienie lub uniemożliwienie odegrania przez Polskę istotnej roli w sytuacji kryzysowej i zakłócenie działań koalicyjnych prowadzonych na terytorium Polski. Oddziaływanie to może mieć również na celu wymuszenie pożądanego przez Rosję zachowania w innych aspektach polityki, zwłaszcza w zakresie importu surowców energetycznych. Jednak cały czas celem długofalowym byłoby wykazanie nieefektywności NATO i UE oraz odsunięcie od granic Rosji wojsk zachodnich. W jeszcze dłuższej perspektywie oznaczałoby to możliwość ułożenia relacji politycznych i gospodarczych z państwami Europy Zachodniej na warunkach korzystnych dla Rosji.

W takim kontekście geopolitycznym zamachy z użyciem urządzeń wybuchowych mogą mieć na celu zarówno osłabienie struktur państwa, jak również skomplikowanie sytuacji wewnętrznej, zatem możliwe są oba wspomniane powyżej rodzaje ataków.

W grupie pierwszej, mając na uwadze kontekst geopolityczny, można ocenić, że celem ataków będą najprawdopodobniej obiekty infrastruktury krytycznej oraz obiekty wojskowe. Wśród obiektów infrastruktury krytycznej, za najbardziej prawdopodobne można uznać:

- system zaopatrzenia w energię, surowce energetyczne i paliwa,
- system transportowy, służący zarówno do transportu drogowego, kolejowego, morskiego, jak i lotniczego,
- systemy łączności i sieci teleinformatyczne.

Uderzenie w te trzy systemy może spowodować poważne zakłócenie funkcjonowania państwa i utrudnić przemieszczanie się sił wzmocnienia oraz własnych sił zbrojnych w razie wystąpienia poważnego kryzysu. Przykładowo istnieje

[2] Zwraca się tu uwagę zwłaszcza na tzw. przesmyk suwalski, czyli pogranicze Polski i Litwy. Jest to jedyny lądowy łącznik pomiędzy państwami bałtyckimi a resztą NATO, a także możliwy kierunek działań rosyjskich nakierowanych na ustanowienie lądowego połączenia pomiędzy Obwodem Kaliningradzkim a Rosją (via Białoruś).

obecnie dziesięć linii kolejowych łączących Polskę z Niemcami, które mogą zostać wykorzystane do transportu uzbrojenia (w tym ciężkiego sprzętu wojskowego) i zaopatrzenia [Mapa Interaktywna Linii Kolejowych]. Wszystkie prowadzą do jednego z węzłów kolejowych: Szczecin, Krzyż Wielkopolski, Kostrzyń, Rzepin, Czerwieńsk, Żagań, Węgliniec. Dalej na zachód ważną rolę w ruchu kolejowym odgrywają takie węzły jak: Wrocław, Leszno, Ostrów Wielkopolski, Poznań, Białogard, Chojnice, Bydgoszcz czy Tczew.

Umieszczenie urządzeń wybuchowych, niszczących tory (a w optymalnym scenariuszu także tory wraz z przejeżdżającym po nich taborem), sieć trakcyjną na liniach zelektryfikowanych, urządzenia sterowania ruchem kolejowym w sposób skoordynowany, nawet tylko na części linii lub tylko w niektórych węzłach, mogłoby sparaliżować transport kolejowy na znacznym obszarze kraju. Potencjalne spore zakłócenia mogłoby spowodować samo tylko zniszczenie w wielu miejscach elementów sieci trakcyjnej – np. samych słupów[3] lub, wymagające większych środków, podstacji trakcyjnych [Górowski 2019]. Nawet po szybkim udrożnieniu torów, do momentu odbudowy sieci trakcyjnej ruch transportów byłby utrudniony z uwagi na dominację liniowych lokomotyw elektrycznych w taborze PKP Cargo i innych przewoźników kolejowych w Polsce[4].

Odpowiednie zgranie takich działań z akcją informacyjną i polityczną mogłoby mieć daleko idące konsekwencje dla efektywności reakcji NATO na kryzys w otoczeniu Polski. W odpowiedzi na działania o charakterze militarnym (przerzut sił wzmocnienia) Rosja zaatakowałaby polską i zachodnią opinię publiczną zdjęciami zatrzymanych na szlakach lub na przypadkowych stacjach transportów wojskowych. Do tego należy dodać zakłócenia gospodarcze (także w transporcie pasażerskim) wywołane atakami na linie kolejowe.

Zakłócenia byłby jeszcze większe, gdyby celem ataku nie była sieć kolejowa ale sieć energetyczna jako taka. W szczególności podatna na atak może być sieć przesyłowa najwyższych i wysokich napięć. Podobnie jak w przypadku sieci kolejowej, linie przesyłowe są trudne do bieżącego nadzoru. Słupy sieci są zestandaryzowane co ułatwia przygotowanie odpowiednich urządzeń wybuchowych. Ponadto, jeśli za atakiem stałoby obce państwo, możliwe byłoby wcześniejsze przygotowanie odpowiednich urządzeń w formie łatwej do szybkiego umieszczenia na atakowanych

[3] Słupy sieci są w tym przypadku najtrudniejszym do ochrony elementem sieci, z racji ich rozproszenia na długości całego zelektryfikowanego odcinka

[4] Większość taboru spalinowego w Polsce to lokomotywy przeznaczone do pracy manewrowej lub prowadzenia lekkich pociągów towarowych , ciężkie lokomotywy (np. serii ST44) są podczas normalnej eksploatacji rozproszone po Polsce, głównie na szlakach niezelektryfikowanych

obiektach. Z punktu widzenia politycznego najbardziej efektywną opcją byłoby przerwanie dostaw energii do jednej dużej aglomeracji, niszcząc symultanicznie jak najwięcej (optymalnie – wszystkie) linii przesyłowych. Brak prądu oznaczałby unieruchomienie części transportu zbiorowego, wstrzymanie pracy zakładów produkcyjnych, brak dostępu do handlu i usług (nie działające bankomaty, kasy fiskalne i inne urządzenia), zakłócenia w pracy systemów telekomunikacyjnych i inne zakłócenia normalnego funkcjonowania wielu podmiotów. Skalę problemów dobrze ilustruje awaria sieci przesyłowych do której doszło w roku 2008 w Szczecinie, spowodowana zjawiskami naturalnymi (silny wiatr i duże opady śniegu) [Raport Zespołu ds. Zbadania Przyczyn i Skutków Katastrofy Energetycznej 2008].

Zademonstrowanie możliwości pozbawienia dużej aglomeracji, takiej jak wrocławska czy poznańska, zasilania w energię elektryczną, wywołania destabilizacji lokalnej (i nie tylko) gospodarki, przy zastosowaniu odpowiednich narzędzi propagandowych, eksponujących drastyczne zdarzenia, do których doszłoby w takiej sytuacji (lub rozpowszechniając odpowiednio przygotowane fałszywe wiadomości) pozwala wręcz na wywołanie ogólnokrajowej paniki. Wystarczyłoby zasugerować – choćby przez pojedynczy atak w innym miejscu – że możliwe jest powtórzenie tego scenariusza w innych aglomeracjach.

Jest to jednak scenariusz o tyle optymistyczny, że przy wykorzystaniu wszystkich dostępnych narzędzi prawnych (ze stanami wyjątkowymi włącznie) oraz zasobów służb policyjnych, ratowniczych, wojska oraz innych podmiotów (w tym przedsiębiorstw) możliwe jest przynajmniej częściowe opanowanie sytuacji. Trudno jednak oszacować, na ile konieczność zaangażowania tych sił i środków (w tym oddziałów zwartych Policji, pododdziałów wojska, sprzętu transportowego i inżynieryjnego, rezerw strategicznych). Trzeba jednak mieć na uwadze, że ich użycie może ograniczyć lub wręcz wykluczyć możliwość reakcji na inne zagrożenia, co ma oczywiste skutki polityczne.

Inny możliwy scenariusz dotyczy ataku wymierzonego nie w ludność, ale w transport morski. Mimo że Morze Bałtyckie jest morzem niewielkim, to jednak jego znaczenie gospodarcze i militarne dla bezpieczeństwa Polski jest duże. W roku 2017 przeładowano w portach polskich osiemdziesiąt siedem milionów ton ładunków, w tym drobnicę oraz paliwa [Actia Forum 2018]. Możliwość importu i eksportu wyrobów przemysłowych i dóbr konsumpcyjnych ma zasadnicze znacznie dla stabilności polskiej gospodarki, opartej na sieciach powiązań z gospodarkami innych państw, natomiast dostawy surowców energetycznych (ropa naftowa i gaz ziemny) mają fundamentalne znaczenie jako alternatywa dla dostaw z Rosji.

Atak z użyciem urządzeń wybuchowych umieszczonych na szlakach żeglugowych na Bałtyku może być szczególnie efektywny właśnie w sytuacji zastosowania wobec Polski szantażu energetycznego. Urządzenia te mogą zostać rozmieszczone na dnie morza w sposób skryty, przy użyciu okrętów podwodnych lub zmodyfikowanych cywilnych jednostek nawodnych (handlowych, badawczych, rybackich lub jachtów). Możliwe jest wykorzystanie do tego celu także bezzałogowych pojazdów podwodnych. Istnieje również możliwość użycia płetwonurków bojowych, choć z uwagi na możliwości środków technicznych jest to mniej prawdopodobna opcja. Przykładowo pojazdy podwodne z rodziny Hugin [Dąbrowski 2019] są w stanie operować autonomicznie, zgodnie z zadanym programem przez okres od dwudziestu czterech do sześćdziesięciu godzin, wykorzystując inercyjny system nawigacyjny. Bezzałogowe, autonomiczne pojazdy podwodne są to przy tym urządzeniami szeroko wykorzystywanymi w przemyśle wydobywczym i badaniach oceanograficznych, więc pozyskanie komercyjnie dostępnych urządzeń i ich modyfikacja w celach bojowych jest łatwa dla takiego państwa jak Rosja [Sutton 2018]. Użycie pojazdów pochodzenia zachodniego może przy tym zapewnić warunek wiarygodnego zaprzeczenia.

Także same urządzenia wybuchowe mogą cechować się wysokim poziomem zaawansowania technicznego. We współczesnej walce morskiej rzeczą normalną jest wyposażenie min w sensory akustyczne, które wraz z bazą sygnatur (charakterystyk dźwiękowych) potencjalnych celów mogą, zamaskowane na dnie, oczekiwać jednostki określonego typu. Możliwe jest więc przykładowo takie zaprogramowanie miny ustawionej na podejściu do Świnoujścia, aby ignorowała promy czy masowce, ale eksplodowała w momencie wykrycia zbiornikowca zmierzającego w kierunku terminala gazowego. Co więcej miny morskie mogą zostać postawione z dużym wyprzedzeniem czasowym, przykładowo jedna z min oferowanych przez rosyjski przemysł zbrojeniowy może pozostawać w gotowości przez co najmniej rok [Rosobronoexport 2018]. Może także mieć miejsce przymocowanie urządzenia wybuchowego bezpośrednio do kadłuba wybranego statku, przy pomocy płetwonurków lub pojazdów podwodnych.

Należy pamiętać, że uderzenie w transport surowców energetycznych jest groźne z wielu powodów. Zniszczenie zbiornikowca przewożącego ropę naftową oznacza katastrofę ekologiczną (i wymierne straty finansowe, choćby dla turystyki) i uniemożliwienie na dłuższy czas normalnej żeglugi na znacznej części południowego Bałtyku. Jeszcze gorsze są skutki zniszczenia gazowca. Skutki eksplozji takiej jednostki są porównywalne z eksplozją nuklearną, pomijając oczywiście skażenie radioaktywne. Mowa bowiem o eksplozji, która, jak wykazały badania

Sandia National Laboratory, spowodować może zapłon papieru w odległości do pięciuset metrów, a oparzenia drugiego stopnia u ludzi w odległości półtora kilometra [Sandia National Laboratory 2004]. Zniszczenia mogą być jednak dużo większe, jeśli gaz po wycieku nie zacznie płonąć natychmiast, a będzie się ulatniać, tworząc mieszankę wybuchową, do detonacji której dojdzie po pewnym czasie. Wtedy zagrożony jest obszar do trzech i pół kilometra. Oczywiście zniszczenia w mieniu będą jeszcze większe, gdy dojdzie do eksplozji wtórnych, na przykład kolejnych zbiorników gazu[5].

Atak tego rodzaju jest szczególnie groźny, gdy zostanie powiązany z działaniami ekonomicznymi (odcięcie przez Rosję dostaw surowców energetycznych na przykład pod pozorem problemów technicznych) i informacyjnymi. Spowodowanie zagrożenia dla żeglugi, może zostać łatwo zdyskontowane propagandowo jako zagrożenie ekologiczne, a jako sprawcy ataku mogą zostać wskazani radykalni ekolodzy. Możliwe jest wtedy wykorzystanie zachodniej opinii publicznej i wywarcie przez nią nacisku na wstrzymanie dalszych dostaw surowców energetycznych do Polski drogą morską. Ponadto możliwe jest przejście do otwartego użycia sił zbrojnych poprzez wyprowadzenie rosyjskich sił morskich na Bałtyk w charakterze swoistych sił stabilizujących – jak wskazuje kmdr M. Matuszewski [2016]. Rosja mogłaby uzasadnić taki krok brakiem zdolności państwa polskiego do zapewnienia bezpieczeństwa żeglugi.

Niestety należy przy tym zauważyć, że obecnie polskie możliwości przeciwdziałania takim zagrożeniom są ograniczone. Marynarka Wojenna posiada w chwili pisania tego tekstu w 13. Dywizjonie Trałowców trzy niszczyciele min projektu 206FM i jeden projektu 258 („ORP Kormoran") mogące wykrywać, klasyfikować i zwalczać miny morskie dzięki szerokiej gamie środków technicznych, w tym pojazdów podwodnych lub poprzez zaokrętowanych płetwonurków-minerów. Dużo liczniejsze (aż 17 okrętów) trałowce bazowe projektu 207 eksploatowane w 12. i 13. Dywizjonie Trałowców mają w tym zakresie mniejsze możliwości (są to jednostki przede wszystkim przeznaczone do klasycznego trałowania min kontaktowych i niekontaktowych)[6]. Do tego w składzie obydwu dywizjonów znajdują się Grupy Płetwonurków-Minerów. Sytuacja w tym zakresie jest o tyle dobra, że w składzie

[5] Na przykład kolejnych gazowców lub zbiorników terminala LNG. Warto w tym momencie przywołać powieść autorstwa byłego analityka marynarki wojennej USA, L. Bonda, pt. „Kocioł". Opisano w niej szczegółowo atak na gazowiec stojący w Zatoce Gdańskiej, który skutkuje wtórną detonacją dwóch kolejnych jednostek tego rodzaju, z katastrofalnymi dla Trójmiasta rezultatami.

[6] Aczkolwiek możliwe jest z ich pokładów operowanie lekkimi pojazdami podwodnymi (typu Gavia), mogą także przewozić płetwonurków-minerów.

sił przeciwminowych w ciągu najbliższych lat znajdą się kolejne dwa nowoczesne niszczyciele min projektu 258, co pozwoli zastąpić okręty 206FM.

Dużo gorsza sytuacja panuje w zakresie sił zwalczania okrętów podwodnych. Dwie fregaty, jedna korweta, trzy okręty podwodne uzupełnione przez śmigłowce Mi-14PŁ i SH-2G to zbyt małe siły, zwłaszcza gdy weźmie się po uwagę, że trapione różnymi problemami technicznymi, nie są w stanie efektywnie kontrolować sytuacji na Bałtyku. Trzeba mieć przy tym na uwadze, że okręty podwodne (jak również bezzałogowe pojazdy podwodne) mają kluczowe znaczenie dla prowadzenia rozpoznania i wspierania działań dywersyjnych, a rozpoznanie może być prowadzone na długo przed podjęciem działań. W przypadku Morskiego Oddziału Straży Granicznej, posiada on wyłącznie jednostki typowo patrolowe, w większości kutry, łodzie motorowe i poduszkowce. Ponadto wobec problemów związanych z ilością i możliwościami śmigłowców poszukiwawczo-ratowniczych, problematyczne może być także efektywne reagowanie na sytuacje kryzysowe na morzu. Skuteczne przeciwdziałanie zagrożeniom hybrydowym wymaga więc daleko idącej modernizacji sił okrętowych i lotnictwa morskiego oraz sił Straży Granicznej.

Spośród możliwych sytuacji ataku na infrastrukturę krytyczną oraz obiekty wojskowe i policyjne, należy zwrócić także szczególną uwagę na możliwość wykorzystania jako nośników urządzeń wybuchowych bezzałogowych statków latających (dronów). Mogą to być pojazdy dostępne komercyjnie, zmodyfikowane pod kątem wykonania danego zadania lub też urządzenia zbudowane od podstaw. Można ich użyć do jednorazowego ataku lub tylko przemieścić (zrzucić) na cel przenoszony przez nie ładunek. Ich użycie pozwala ominąć naziemne systemy ochrony i możliwe jest przy okazji pozyskanie dobrej jakości zdjęć, co może mieć wymiar propagandowy. Warto zauważyć, że podobne zdarzenie miało już miejsce w roku 2015, gdy nad wojskową część lotniska Kraków–Balice wleciał bezzałogowiec, z którego pokładu zrzucono flarę [JK 2015]. Możliwe jest także użycie bezzałogowych statków powietrznych do innych zadań, zarówno rozpoznawczych, jak również dezorganizacji ruchu lotniczego (także na lotniskach wojskowych).

W zakresie drugiej grupy ataków, mających charakter prowokacji politycznej, szczególnie atrakcyjnym celem mogą być masowe zgromadzenia, takie jak demonstracje, uroczystości podczas świąt państwowych, ceremonii religijnych oraz wizyt przywódców obcych państw i obrad organizacji międzynarodowych. W tym przypadku atak może być mało wyrafinowany pod względem technicznym i mogą być użyte improwizowane urządzenia wybuchowe. Atakowi będzie towarzyszyć odpowiednio przygotowany przekaz medialny, sugerujący że sprawcami są osoby powiązane z jedną z miejscowych faktycznie działających organizacji politycznych

(skrajnie lewicowych lub prawicowych). Możliwy jest też scenariusz, w którym do zamachu zostanie dopasowana narracja sugerująca, że za zdarzeniem stoją polskie lub zagraniczne służby specjalne lub osoby z nimi związane, sugerując w ten sposób działanie przeciwko opozycji. Możliwych scenariuszy tego rodzaju jest wiele, ale można ocenić, że będą się one mieścić w kliku obszarach konfliktów.

Przede wszystkim, możliwe jest uderzenie wykorzystujące konflikt pomiędzy dwiema częściami polskiego społeczeństwa – bardziej konserwatywną, z reguły głosującą na partie konserwatywno-prawicowe, manifestującą swoją religijność i tą liberalną, głosującą na partie lewicowe i liberalne, sceptyczną wobec religii. Można sądzić, że ten konflikt, stanowiący obecnie fundament podziałów socjopolitycznych w Polsce będzie istotny przez wiele lat. Nietrudno wyobrazić sobie sposób na jego zaostrzenie – eksplozja bomby podczas Parady Równości, do której przyzna się organizacja nacjonalistyczna czy zamach podczas obchodów 11 listopada za którą medialną odpowiedzialność weźmie na siebie organizacja skrajnie lewicowa. Podobnie podatne na rozniecenie się inne spory, w tym potencjalnie także etniczne związane z napływem do Polski dużej liczby osób narodowości ukraińskiej lub sporów dotyczących historii stosunków polsko-żydowskich i polsko-niemieckich. Należy mieć przy tym na uwadze, że celem ataku nie muszą być koniecznie wydarzenia tradycyjnie uważane za wymagające szczególnej ochrony, jak np. uroczystości z udziałem przywódców państw. Będą to wszystkie imprezy, uroczystości demonstracje i tym podobne wydarzenia przyciągające uwagę opinii publicznej. Nie muszą być one organizowane przez skrajnie lewicowe lub prawicowe organizacje. Możliwe jest, że celami zamachów będą konkretne osoby, symbolizujące określone opcje polityczne lub ideologiczne, ale niekoniecznie sprawujące w danym momencie funkcje państwowe. Przeciwnie, rola symboliczna jest często większa w przypadku osób, które takie funkcje sprawowały w przeszłości. Nie można także wykluczyć, ze celami ataków będą media, zarówno ich siedziby, jak i dziennikarze.

Podsumowanie

Opisane powyżej problemy ilustrują całokształt zagadnień związanych z zagrożeniem użyciem podczas wojny hybrydowej urządzeń wybuchowych w różnych formach.

Spośród nich należy wymienić:

1) Ataki z użyciem urządzeń wybuchowych będą dobrze przygotowane pod kątem wywiadowczym, logistycznym i technicznym. Jest możliwe, że

przygotowania te będą prowadzone – zwłaszcza w wymiarze wywiadowczym – na wiele lat przed zaistnieniem sytuacji, w której mogłoby dojść do użycia siły. Oznacza to konieczność zwracania szczególnej uwagi, zwłaszcza w aspekcie ochrony infrastruktury krytycznej, na ochronę przed obcymi działaniami wywiadowczymi.

2) Zamachy z użyciem urządzeń wybuchowych będą dokonywane w sposób zaplanowany przez osoby posiadające odpowiednie przeszkolenie, być może także doświadczenie praktyczne i znające techniki i procedury działań minersko-pirotechnicznych. Możliwe jest więc użycie urządzeń wybuchowych szczególnie trudnych do wykrycia i neutralizacji.

3) Bezpośredni sprawcy zamachów będą mogli wykorzystać szereg środków ułatwiających im przeprowadzenie ataku. Działając ze wsparciem struktur wywiadowczych, będą mogli na przykład łatwo udawać osoby, których obecność w danym miejscu nie budzi wątpliwości. Przykładowo mogą udawać personel techniczny, serwisowy. Nie chodzi tu tylko o samo proste przebranie się ale o to, że na użytek działalności wywiadowczej i dywersyjnej mogą zostać wręcz utworzone lub zinfiltrowane faktycznie działające podmioty gospodarcze.

4) Jest także możliwe, że zamachowcy będą w fazie przygotowań lub samego zamachu wykorzystywać osoby podające się za dziennikarzy. Często osoby akredytowane jako dziennikarze – a w praktyce będące freelancerami lub blogerami nie związanymi z żadnym tradycyjnym medium – uzyskują dostęp do obiektów wojskowych i osób się tam znajdujących. Jest to wyzwanie zarówno dla służb ochrony, jak i służb prasowych.

5) Zamachy mogą być przeprowadzone z użyciem szeregu środków technicznych, w tym bezzałogowych statków latających i pojazdów podwodnych. Możliwe jest także sięgnięcie po inne środki techniczne, umożliwiające umieszczenie w pożądanym przez sprawców miejscu urządzenia wybuchowego oraz nagranie obrazu jego detonacji i spowodowanych przez nią skutków.

6) Reagowanie na zamachy z użyciem urządzeń wybuchowych wymaga użycia znacznych sił i środków znajdujących się w dyspozycji Policji, Krajowego Systemu Ratowniczo-Gaśniczego, Sił Zbrojnych oraz cywilnych struktur administracji publicznej, samorządowej oraz podmiotów gospodarczych.

7) Nieodłączną częścią zapobiegania i reagowania na te zagrożenia jest prowadzenie aktywnej działalności informacyjnej, wpływającej skutecznie na postawy opinii publicznej i przeciwdziałającej dezinformacji ze strony przeciwnika.

Należy przy tym mieć na uwadze, że działania te mogą mieć charakter wykraczający poza samo tylko użycie urządzeń wybuchowych i mogą również

manifestować się w formie sytuacji zakładniczych, zwłaszcza uprowadzeń osób, co zasługuje na odrębne omówienie.

Bibliografia

Actia Forum (2018), *Polskie porty w 2017 – padły rekordy* (raport) [online], http://www.gospodarkamorska.pl/Porty,Transport/polskie-porty-w-2017---padly-rekordy-rekord-actia-forum.html, dostęp: 10.07.2018.

Barno D., Benshel N. (2015), *Fighting And Winning In The "GRAY Zone"* [online], https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/, dostęp: 3.07.2018.

Chambers J. (2016), *Countering Gray-Zone Hybrid Threats An Analysis of Russia's New Generation Warfare' and Implications for the US Army*, West Point, Washington.

Cullen P., Reichborn-Kjennerud E. (2017), *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare* [online], https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf, dostęp: 3.07.2018.

Dąbrowski K. (2019), *Hugin 1000 MR*, „Frag Out!", nr 24, ss. 30–37.

Górowski M. (2019), *Sieć trakcyjna 3kV DC* [online], http://www.transportszynowy.pl/trakcjazasilanie.php, dostęp: 09.07.2018.

Hoffman F. (2009), *Hybrid vs Compound War*, „Armed Forces Journal", October 1 [online], http://armedforcesjournal.com/hybrid-vs-compound-war/, dostęp: 3.07.2018.

JK (2015), *Dron zrzucił ładunek wybuchowy na lotnisko w Balicach? ABW prowadzi śledztwo* [online], http://www.newsweek.pl/polska/dron-nad-lotniskiem-w-balicach-czy-zrzucil-ladunek-wybuchowy-,artykuly,367358,1.html, dostęp: 11.07.2018.

Kubiak K., Makowski A. (1998), *Terroryzm jako sposób prowadzenia wojny?*, „Raport – wojsko technika obronność", 4, ss. 41–43.

Ludność. Stan i struktura demograficzno-społeczna. Narodowy Spis Powszechny Ludności i Mieszkań (2011) [online], http://stat.gov.pl/cps/rde/xbcr/gus/LUD_ludnosc_stan_str_dem_spo_NSP2011.pdf, dostęp: 8.07.2018.

Mapa Interaktywna Linii Kolejowych [online], http://mapa.plk-sa.pl, dostęp: 9.07.2018.

Matuszewski M. (2016), *Niebieskie ludziki. Wojna morska na Bałtyku nie jest nierealna* [online], https://wszystkoconajwazniejsze.pl/maciej-matuszewski-niebieskie-ludziki-wojna-morska/, dostęp: 10.07.2018.

„Przegląd Bezpieczeństwa Wewnętrznego" (2015), Wydanie specjalne – wojna hybrydowa [online], https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html, dostęp: 03.07.2018.

Raport Zespołu ds. Zbadania Przyczyn i Skutków Katastrofy Energetycznej (2008), [online], http://www.szczecin.uw.gov.pl/systemfiles/articlefiles/1466/(20111202.120000).raport_koncowy-czesc_-1.pdf, dostęp: 8.07.2018.

Rosobronoexport (2018), *MDM-3 Sea bottom mine (Mod.1)* [online], http://roe.ru/eng/catalog/naval-systems/shipborne-weapons/mdm-3, dostęp: 10.08.2018.

Sandia National Laboratory (2004), *Guidance on Risk Analysis and Safety Implications of a Large Liquefied Natural Gas (LNG) Spill Over Water* [online], https://regulatorwatch.com/wp-content/uploads/2015/08/2004-12_SANDIA-DOE_RISK_ANALYSIS.pdf, dostęp: 10.08.2018.

Sutton H.I. (2018), *British deep-sea robot seen on Russian GUGI ship passing UK* [online], http://www.hisutton.com/Yantar_News.html, dostęp: 10.08.2018.

Andrzej Więcławski | andrzej2103@onet.eu
Społeczna Akademia Nauk

Społeczne aspekty udziału Sił Zbrojnych RP w misjach i operacjach poza granicami kraju w kontekście bezpieczeństwa międzynarodowego

Wstęp

Jednym z trzech rodzajów misji realizowanych przez Siły Zbrojne Rzeczypospolitej Polskiej, oprócz zapewnienia obrony kraju i przeciwstawienia się agresji zbrojnej oraz wspierania bezpieczeństwa wewnętrznego i pomocy społeczeństwu, jest udział w procesie stabilizacji sytuacji międzynarodowej. Polscy żołnierze realizują tę misję, biorąc czynny udział w misjach i operacjach poza granicami kraju w różnych częściach świata. Zwolennicy naszego zaangażowania w misje zagraniczne twierdzą, że udział Sił Zbrojnych RP ma zawsze określone cele militarne i polityczne, które w mniejszym lub większym stopniu przyczyniają się do podniesienia poziomu bezpieczeństwa narodowego oraz umacniają pozycję państwa na arenie międzynarodowej.

Celem artykułu jest przedstawienie zróżnicowanego postrzegania w społeczeństwie służby polskich żołnierzy w misjach i operacjach poza granicami kraju. Zaprezentowane poniżej opinie oparte będą głównie na wiedzy autora oraz jego doświadczeniu zawodowym żołnierza-weterana poszkodowanego, wyniesionym z udziału w trzech misjach – UNIFIL w Libanie, SFOR w Bośni i Hercegowinie oraz Iraqi Freedom w Iraku. Autor przedstawił wizerunek polskiego żołnierza, który wyjeżdżając na misje, wykonując powierzone zadania, narażał własne zdrowie i życie dla światowego bezpieczeństwa. Niniejszy artykuł przybliży potrzebę dyskusji na temat postrzegania w społeczeństwie żołnierza-uczestnika misji i jego roli w zapewnieniu bezpieczeństwa międzynarodowego. Autor artykułu, jako żołnierz-uczestnik misji, stara się szerzyć tę tradycję oraz kształtować świadomość społeczną w tym zakresie.

Nie istnieje jednolita polska definicja misji stabilizacyjnej. Przyjmuje się, że misje tego typu nie ograniczają się jedynie do zadań wojskowych. Są to misje kompleksowe, wieloaspektowe, obejmujące oprócz zadań wojskowych również kwestie polityczne, ekonomiczne, społeczne oraz kulturowe, niemniej jednak kluczowa jest współpraca cywilno-wojskowa, określana jako CIMIC (*Civil-military Cooperation*) [Jureńczyk 2016, s. 229].

Zgodnie z terminologią Sojuszu Północnoatlantyckiego (*North Atlantic Treaty Organization* – NATO) celem tzw. misji (operacji) wsparcia pokoju może być:

- zapobieganie konfliktom (*conflict prevention*),
- tworzenie pokoju (*peace making*),
- utrzymanie pokoju (*peacekeeping*),
- wymuszanie pokoju (*peace enforcement*),
- budowanie pokoju (*peacebuilding*),
- pomoc humanitarna (*humanitarian aid*) [Jureńczyk 2016, s. 229].

Z kolei ONZ definiuje operacje pokojowe jako siły pokojowe ONZ, które to są częścią sił zbrojnych państwa oddanych do dyspozycji ONZ w celu przeprowadzenia konkretnych misji pokojowych. Z założeń ONZ wynika, że siły pokojowe stanowią nieprzymusowy instrument kontroli konfliktów zbrojnych [https://encyklopedia.pwn.pl/haslo/sily-pokojowe-ONZ;3975308.html].

Polski Kontyngent Wojskowy (PKW) to wydzielona jednostka Sił Zbrojnych Rzeczypospolitej Polskiej, przeznaczona do udziału w operacji wojskowej o charakterze wojennym, pokojowym lub stabilizacyjnym poza granicami kraju. Decyzję o wysłaniu PKW za granicę wydaje Prezydent RP na wniosek Rady Ministrów. Organizacyjnie PKW podlega Ministrowi Obrony Narodowej, a operacyjnie dowództwu wyznaczonemu w postanowieniu o użyciu PKW, jednak w praktyce jest to wspólne dowództwo wyznaczone przez organizację, pod której auspicjami prowadzona jest dana misja [Jureńczyk 2016, s. 229].

Polscy żołnierze uczestniczą w misjach poza granicami na rzecz wygaszania konfliktów i przywracania bądź utrzymania pokoju od 1953 r., kiedy to po raz pierwszy zostali wysłani do Korei w celu nadzorowania zawieszenia broni między republikami koreańskimi, aż do chwili obecnej, gdy służą pod auspicjami ONZ, UE i NATO.

Dobrze postrzegana przez społeczeństwo była misja UNIFIL w Libanie pod auspicjami ONZ. Polską obecność w Libanie traktowano jako bardzo cenną, a Polska miała opinię jednego z większych i bardziej solidnych partnerów. Polscy żołnierze w ramach tej misji, poza zadaniami mandatowymi, udzielali także w szerokim zakresie pomocy humanitarnej mieszkańcom południowego Libanu. Dzięki udziałowi w tej misji polscy żołnierze zdobyli doświadczenie w realizacji zadań nie tylko

logistycznych, ale także operacyjnych w trudnych warunkach terenowych i klimatycznych. Jednak należy pamiętać, że misje ONZ w większości refundowane były z budżetu Narodów Zjednoczonych.

Przez wiele lat polscy żołnierze w warunkach wielonarodowych grup bojowych mogli zdobywać doświadczenie w dowodzeniu, planowaniu, działaniach operacyjnych, jak i szeroko pojętej logistyce. Weterani tych misji, którzy później uczestniczyli w Polskim Kontyngencie Wojskowym w Iraku i Afganistanie, o wiele szybciej odnaleźli się w nowych, cięższych, bo w wojennych, warunkach służby. W Polsce istnieje przekonanie, że wojskowe zaangażowanie daleko poza granicami kraju wzmacnia bezpieczeństwo naszego kraju oraz daje rękojmię bezpieczeństwa w przyszłości.

Pomimo wspomnianej funkcji gwarancyjnej, jaką pełnią misje stabilizacyjne, w ciągu przeszło sześćdziesięciu lat ewoluował zarówno charakter konfliktów zbrojnych, jak i misji oraz operacji prowadzonych w ich rezultacie. Wpłynęło to znacząco na zintensyfikowanie pojawiania się wyzwań i zagrożeń dla żołnierzy biorących w nich udział, a co za tym idzie, dostrzeżenie szeregu problemów związanych z tym zagadnieniem [Krzemińska 2016, s. 106]. Jednym z nich są relacje żołnierz-weteran działań poza granicami państwa a najbliższe otoczenie społeczne, z którego pochodzi.

Status prawny misji poza granicami kraju

Siły Zbrojne mają za zadanie nie tylko strzec bezpieczeństwa na obszarze prowadzenia operacji, lecz także używać siły zgodnie z przyznanym mandatem i zasadami jej użycia, co oznacza również prowadzenie regularnych działań bojowych. Skutkiem takich działań są ranni, poszkodowani oraz polegli na misjach żołnierze międzynarodowych kontyngentów. Powracającym z misji żołnierzom z uszczerbkiem na zdrowiu psychicznym i fizycznym należy nieść pomoc. Służy temu wprowadzenie regulacji prawnej nadającej tej grupie odrębny status i związane z nim uprawnienia. Pomimo aktywnego zaangażowania Sił Zbrojnych w działania na rzecz światowego pokoju Polska długo pozostawała jedynym krajem NATO, w którym brakowało regulacji prawnej dotyczącej uczestników misji poza granicami państwa. Pierwszy akt prawny regulujący służbę polskich żołnierzy poza granicami kraju – Ustawa z 19 lutego 1998 roku o zasadach użycia lub pobytu Sił Zbrojnych Rzeczypospolitej Polskiej poza granicami państwa, weszła w życie w 1998 r., co oznacza, że przez prawie pół wieku (misje SZ RP datuje się od 1953 roku) polscy żołnierze nie mieli

żadnych uprawnień z tytułu uczestnictwa w misjach. Priorytetem polskiego rządu stało się unormowanie statusu prawnego uczestników misji oraz wprowadzenie szeregu uprawnień dla weteranów, ich rodzin oraz rodzin poległych żołnierzy. Ostatecznie rząd polski uregulował tę kwestię poprzez uchwalenie 19 sierpnia 2011 roku ustawy o weteranach działań poza granicami państwa[1], która weszła w życie 30 marca 2012 roku. Ustawa ta określa status weterana oraz weterana poszkodowanego oraz warunki, zasady i tryb przyznawania oraz korzystania z tych uprawnień. Zasadną powinnością państwa jest pomoc tym wszystkim żołnierzom, którzy mają status weterana bądź weterana poszkodowanego, poprzez unormowanie ich statusu prawnego i readaptacji do życia w społeczeństwie. Takim żołnierzom, którzy doznali uszczerbku na zdrowiu fizycznym albo psychicznym, należy się pomoc ze strony państwa, gdyż wykonywali oni swoje obowiązki, reprezentując Polskę poza jej granicami.

Społeczeństwo wobec służby polskich żołnierzy poza granicami kraju

Militarna obecność Polski poza jej granicami zawsze była tematem żywych dyskusji polskiego społeczeństwa. Życie Polaków uczestniczących w misjach poza granicami kraju to jednak temat mało znany. Społeczeństwo niewiele wie o różnych aspektach życia żołnierzy biorących udział w misjach.

Kiedy skutki uczestnictwa w misjach i operacjach poza granicami kraju zaczęły być odczuwalne na dużą skalę i zaczęły dotyczyć nie tylko samych żołnierzy, ale także społeczeństwa, wzrosła liczba aspektów, przez pryzmat których można oceniać skutki służby polskich żołnierzy w misjach. Faktem jest, że wyobrażenia na ten temat najczęściej są kreowane przez media (telewizję, radio, Internet oraz prasę). To właśnie środki masowego przekazu są głównym inspiratorem oceny przez społeczeństwo udziału polskich żołnierzy w międzynarodowych operacjach wojskowych. Problem militarnej obecności Polski poza jej granicami znajduje się w centrum zainteresowania polskiego społeczeństwa [Krzemińska 2016, s. 106].

Przeanalizowanie popularnych czasopism, publikacji w Internecie dotyczących Polskich Kontyngentów Wojskowych, portali społecznościowych czy serwisów informacyjnych pozwala wyciągnąć wniosek, że kreują one, najogólniej

[1] Ustawa z dnia 19 sierpnia 2011 roku o weteranach działań poza granicami państwa [Dz. U. z 2011 r., poz. 1203].

mówiąc, albo pozytywny, albo negatywny wizerunek udziału polskich Sił Zbrojnych w misjach i operacjach wojskowych. Szczególne kontrowersje budziło zaangażowanie polskich wojsk w Polskim Kontyngencie Wojskowym w Iraku oraz Afganistanie. Negatywne oceny uczestnictwa polskich żołnierzy w misjach zaczęły nasilać się wraz ze wzrostem liczby rannych, poszkodowanych oraz poległych polskich żołnierzy w operacji irackiej i afgańskiej. Misje te, uchodzące za pokojowe czy stabilizacyjne, stały się *de facto* operacjami bojowymi. Polskie Kontyngenty okazały się nieprzygotowane do działań *stricte* bojowych tak pod względem sprzętu, jak i norm prawnych oraz przepisów wojskowych. Spadek społecznego poparcia dla działań ekspedycyjnych Sił Zbrojnych był spowodowany również wątpliwościami dotyczącymi zasadności wysyłania polskiego komponentu w te rejony. Przeciwnicy misji uważają, że udział Polaków w operacji w Afganistanie wpływał negatywnie na bezpieczeństwo, gdyż zwiększał zagrożenie atakiem terrorystycznym ze strony muzułmańskich fundamentalistów [Baranowska 2013, s. 10].

Z badań przeprowadzonych w 2010 r. przez Centrum Badania Opinii Społecznej (CBOS) na temat postrzegania przez opinię publiczną zaangażowania Polski w misję w Afganistanie wynikało, że 7% respondentów popierało misję, 79% sprzeciwiało się jej, a 53% badanych wyrażało zdecydowaną dezaprobatę we wszystkich grupach społecznych i demograficznych, niezależnie od poglądów politycznych. [http://www.cbos.pl/SPISKOM.POL/2010/K_159_10.PDF/].

Wraz ze wzrostem zaangażowania Polski w kształtowanie bezpieczeństwa poza granicami rosła liczba zabitych, rannych i poszkodowanych. Misja przyniosła też największe, jak dotąd, straty wśród żołnierzy biorących w niej udział. Jak podaje portal internetowy Wojska Polskiego [http://www.wojsko-polskie.pl/pl/pamieci-poleglych/], zginęło lub zmarło w wyniku odniesionych ran 24 polskich żołnierzy w PKW Irak i 44 w PKW Afganistan, zaś liczba rannych była wielokrotnie wyższa. Śmierć polskich żołnierzy w Iraku i Afganistanie to niewątpliwie tragiczny bilans, którego nie da się zrekompensować w żaden sposób. Straty te przyczyniły się do nasilenia krytyki ze strony opinii publicznej, jak również postawiły pod znakiem zapytania pojęcie misji pokojowej i stabilizacyjnej. Początkowo zakładano, że misja iracka będzie miała charakter typowej misji pokojowej, nikt nie przewidział intensyfikacji działań do stopnia niemal operacji wojennej. Tymczasem kraj stawał się coraz bardziej niebezpieczny, a misja zaczęła tracić swój typowo stabilizacyjny charakter. Negatywne postrzeganie misji polskich żołnierzy w społeczeństwie, oprócz strat w ludziach, warunkowały również straty materialne oraz brak przygotowania żołnierzy polskich kontyngentów do pierwszych zmian

(niewystarczająca ilość wyposażenia, utrudniająca wykonywanie zadań o charakterze bojowym). Błędy logistyczne i proceduralne to tylko niektóre z błędów, trudnych do uniknięcia w tak poważnym przedsięwzięciu. Sondaż przeprowadzony przez Centrum Badania Opinii Społecznej w 2007 r. wskazał, że zdecydowana większość badanych (81%) dystansowała się od udziału polskich żołnierzy w misji stabilizacyjnej w Iraku. Swoje poparcie dla tego przedsięwzięcia deklarował zaledwie co szósty Polak (16%) [http://cbos.pl/SPISKOM.POL/2007/K_162_07.PDF/].

Skutkiem zmiany charakteru współczesnych konfliktów zbrojnych i prowadzonych w ich wyniku operacji jest powstanie nowej grupy społecznej, której zwyczajowo nadaje się miano „weteranów". Obok opisanego powyżej – negatywnego postrzegania w społeczeństwie służby polskich żołnierzy w misjach poza granicami kraju – istnieje również inny – pozytywny sposób postrzegania działań weteranów poza granicami państwa. Wojsko jest częścią społeczeństwa i nie może bez niego istnieć, a spora część społeczeństwa jak dotąd ma pozytywny stosunek do Sił Zbrojnych. To właśnie ten obraz jest coraz bardziej promowany, również przez media oraz przez stowarzyszenia i fundacje działające na rzecz weteranów oraz weteranów poszkodowanych. Ze względu na fakt, że status uczestników misji i operacji poza granicami kraju nie jest uregulowany w międzynarodowym prawie humanitarnym konfliktów zbrojnych, poszczególne państwa we własnym zakresie definiują ich status i uprawnienia. Wprowadzenie w Polsce ustawy o weteranach działań poza granicami państwa zapoczątkowało możliwość stworzenia systemu opieki nad weteranami, właściwe przygotowanie tego procesu, a także ewaluację utylitarnych aspektów jej wdrożenia. Zgodnie z tą ustawą dzień 29 maja jest Dniem Weterana Działań Poza Granicami Państwa (zwanym potocznie „Dniem Weterana"), a zgodnie z uchwałą ONZ jest to Międzynarodowy Dzień Uczestników Misji Pokojowych. W celu uświadomienia społeczeństwu znaczenia poświęcenia polskich weteranów i przeciwdziałania negatywnemu postrzeganiu polskiego uczestnictwa w misjach zorganizowano kampanię społeczną „Dzień Weterana – szacunek i wsparcie". Jej głównym organizatorem jest Stowarzyszenie Rannych i Poszkodowanych w Misjach Poza Granicami Kraju. Ministerstwo Obrony Narodowej, które w pełni zaakceptowało pomysł, współfinansuje opisywane przedsięwzięcie. Świadomość społeczna na temat udziału polskich żołnierzy w misjach poza granicami kraju okazała się na tyle nikła, że jednym z celów Stowarzyszenia stało się jej pogłębianie. Społeczeństwo wciąż niewiele wie o służbie żołnierzy poza granicami kraju, a misje kojarzą się najczęściej z działaniami bojowymi. Kampania pokazała tę bardziej ludzką twarz misji – działania na rzecz lokalnych społeczności, opierające się

przede wszystkim na współpracy cywilno-wojskowej (CIMIC), polegającej głównie na odbudowie zniszczonej w czasie działań zbrojnych infrastruktury drogowej, paliwowej i energetycznej.

Takim pozytywnym działaniem w Dniu Weterana jest przygotowanie billboardów i spotów reklamowych przedstawiających sylwetki uczestników misji stabilizacyjnej w taki sposób, by polskie społeczeństwo zobaczyło trud, jaki ponoszą żołnierze na misjach. Aby ci, którzy powrócili z misji, cieszyli się szacunkiem społecznym i by trwała pamięć o tych żołnierzach, którzy nie wrócili i na zawsze pozostali na polu chwały. Należy stale uświadamiać społeczeństwu, że misje zagraniczne to nie tylko zadania stabilizacyjne, antyterrorystyczne czy bojowe, to także dbanie tam, na miejscu, o rozwój infrastruktury, rozminowanie terenu, szkolenie policji i wojska.

Coroczne centralne obchody Dnia Weterana Działań poza Granicami Państwa, poprzedzone kampanią społeczną „Szacunek i wsparcie", pokazują, że weterani misji to ludzie żyjący, mieszkający wśród lokalnej społeczności, których losy powinny być znane nam wszystkim. Przedsięwzięcie to służy pogłębianiu w polskim społeczeństwie szacunku do polskiego munduru i uwrażliwieniu społeczeństwa na problemy weteranów działań poza granicami państwa i ich rodzin.

Inną akcją społecznościową, która promuje wizerunek weteranów w społeczeństwie, a także zachęca społeczeństwo do pomocy poszkodowanym weteranom, jest „Kawa dla Weterana" – akcja prowadzona na portalu Facebook przez „Fundację Szarik". Jej celem jest zachęcanie do tego, by raz w miesiącu zrezygnować z kubka kawy i przekazać jego równowartość na rzecz polskich weteranów misji międzynarodowych. Pozyskane w ten sposób środki finansowe „Fundacja Szarik" przeznacza na organizowanie dogoterapii dla żołnierzy cierpiących z powodu stresu bojowego (PTSD). Ta kampania i wiele innych na rzecz weteranów skutecznie zmieniła wizerunek żołnierzy weteranów i zachęciła do pomocy poszkodowanym. W dłuższej perspektywie czasu dzięki podobnym kampaniom wielce prawdopodobne jest również wyeliminowanie negatywnego postrzegania przez społeczeństwo udziału Sił Zbrojnych RP w działaniach poza granicami państwa.

W chwili obecnej trwają prace nad nowelizacją ustawy o weteranach, która nie do końca spełniała oczekiwania weteranów, a w szczególności weteranów poszkodowanych, których spora część znalazła się na marginesie życia społecznego. Poważnym krokiem w nowelizowanej ustawie jest poszerzenie pomocy materialnej dla weteranów poszkodowanych w zakresie szkolnictwa, jak również obniżenie kosztów umieszczenia i pobytu w Domu Weterana.

Misje Sił Zbrojnych poza granicami kraju w kontekście profesjonalizacji polskiej armii

Polska jest aktywnym uczestnikiem działań na rzecz pokoju, bezpieczeństwa i stabilizacji międzynarodowej zarówno na europejskim teatrze działań, jak i poza nim. Uczestnictwo w misjach jest źródłem rozwoju, sprawdzianem umiejętności zawodowych żołnierzy, daje także możliwość zdobywania doświadczenia w dowodzeniu międzynarodowymi zespołami o różnym poziomie profesjonalizmu. Dzięki udziałowi PKW w misji w Iraku i Afganistanie w Siłach Zbrojnych RP zaczęły zachodzić zmiany na miarę XXI wieku. Wyznacznikami tej ewolucji stały się między innymi procesy: profesjonalizacji, modernizacji technicznej oraz doskonalenia procesu szkolenia.

Profesjonalizacja Sił Zbrojnych jest konsekwencją zaangażowania polskich żołnierzy w działania poza granicami kraju. Najbardziej znaczące pod tym względem były operacje w Iraku i w Afganistanie, które bezpośrednio przyczyniły się do przyspieszenia transformacji polskiej armii. Ten skutek ekspedycyjnej działalności naszej armii można również uznać za aspekt społeczny, gdyż żołnierze są częścią społeczeństwa, a sama organizacja wojskowa działa niejako dla społeczeństwa, gwarantując zarówno jego bezpieczeństwo narodowe, jak i międzynarodowe [Krzemińska 2016, s. 102].

Również zdaniem Marka Paszkowskiego polityka kadrowa obowiązująca obecnie w Siłach Zbrojnych RP w dużym stopniu uwzględnia doświadczenie nabyte w trakcie służby w strukturach NATO i UE oraz udział w misjach wojskowych. Podkreśla on, że ta nowa jakość w polskiej armii „wpisuje się we współczesne tendencje postrzegania człowieka w organizacji, z uwzględnieniem specyfiki grupy zawodowej, której dotyczy" [Paszkowski 2011, s. 237].

Należy zaznaczyć, że misja w Iraku i Afganistanie znacznie odbiegała od założeń mandatowych, jeśli wziąć pod uwagę kwestię wyposażenia i przygotowania polskiej armii. Krytycznie oceniano wyekwipowanie polskich żołnierzy, nieadekwatne do realiów misji. Problem stanowiły również zasady użycia broni palnej, które zależały od charakteru powierzonej misji. Kolejnym wyzwaniem dla polskich dowódców była współpraca cywilno-wojskowa (CIMIC), która mogła być wykorzystywana jako połączenie zasadniczych celów operacji wojskowej z potrzebami miejscowych społeczności. Dlatego w przygotowaniach do operacji zarówno irackiej, jak i afgańskiej położono duży nacisk na właściwy dobór kadry i jej odpowiednie przygotowanie do kontaktów z miejscową ludnością.

Doświadczenia z udziału w misji irackiej i afgańskiej wpłynęły również pozytywnie na jakość funkcjonowania zabezpieczenia logistycznego Sił Zbrojnych

poprzez poprawę stopnia wyszkolenia personelu logistycznego, zdobywającego doświadczenia w warunkach pola walki. Zebrane tam doświadczenia pozwoliły dokonać zmian w obszarze techniki wojskowej, to znaczy pozyskać nowoczesny sprzęt wojskowy oparty na nowszych technologiach i wprowadzić go do uzbrojenia Sił Zbrojnych Rzeczypospolitej Polskiej [Wolin 2010, s. 116]. Udział PKW w Iraku i Afganistanie przyniósł olbrzymi postęp, jeśli chodzi o wyposażenie żołnierza, zarówno indywidualne, jak i w zakresie sprzętu wykorzystywanego w czasie misji. Pojawiły się nowe samochody terenowe oraz nowoczesne wyposażenie elektroniczne i radiowe. Śmigłowce transportowe i bojowe zostały przystosowane do lotów w różnych warunkach klimatycznych. Na wyposażeniu indywidualnym żołnierzy znalazły się sprzęt noktowizyjny i termowizyjny oraz nowoczesne środki łączności. Można śmiało powiedzieć, że dzięki tym misjom dokonał się olbrzymi skok jakościowy i ilościowy w wyposażeniu stosowanym przez Wojsko Polskie. Miało to miejsce nie tylko w jednostkach biorących udział w operacjach poza granicami kraju, ale *de facto* w całych Siłach Zbrojnych.

W obliczu nowych rodzajów zagrożeń, a zwłaszcza nowego rodzaju konfliktów, wojsko musiało przystosować się do nowych metod i sposobów prowadzenia operacji zagranicznych. Systematyczne doskonalenie procedur współdziałania w ramach układu koalicyjnego w realnych warunkach pola walki wpływa na doskonalenie procedur dowodzenia i kierowania armią. Niewątpliwie udział Sił Zbrojnych w misjach poza granicami kraju pozwolił na zebranie przez nasze wojsko takich doświadczeń, które w dobie aktualnych zmian systemowych w armii są niezbędne do utrzymania dominującej potęgi militarnej i równowagi w sektorze bezpieczeństwa.

Pamiętać należy również, że służba wojskowa jako służba społeczna wymaga szczególnego uspołecznienia – umiejętności współdziałania w układzie zewnętrznym i wewnętrznym [Paszkowski 2011, s. 239]. Dla odpowiedniego rozwoju, a zarazem kształtowania wizerunku organizacji, jaką są przecież Siły Zbrojne, istotny jest szacunek dla tradycji i wartości, na których ta organizacja opierała i opiera swoje istnienie. Wypracowane i przestrzegane wartości organizacyjne mogą okazać się przecież „drogowskazem" dla organizacji, która obecnie jest w trakcie bardzo poważnych zmian. Zarówno zarządzanie zmianą, jak i zarządzanie różnorodnością będzie istotne dla wzmocnienia pozytywnego odbioru roli wojska w zapewnieniu bezpieczeństwa państwa i międzynarodowego. Wartości organizacyjne uznaje się przecież za czynnik motywujący i integrujący członków danej organizacji, wspomagający zarządzanie zmianą, ale jednocześnie wartości te mogą pomóc w pozyskaniu odpowiednich zasobów ludzkich dla organizacji [Stachowicz-Stanusch 2007, ss. 11–33].

Ważne jest także, aby dla potrzeb bezpieczeństwa między społeczeństwem a organizacją – Siłami Zbrojnymi – budowana była współpraca oparta na zaufaniu. Odpowiednia komunikacja, konsultacje publiczne, dialog ze społeczeństwem w celu rozwiązywania problemów oraz wzajemne zrozumienie zarówno obaw społeczeństwa, jak i dążeń, tj. kierunków rozwoju armii, przyczyni się do wzrostu społecznej odpowiedzialności organizacji [Chodyński 2015, ss. 13,19].

Zakończenie

Jedną z podstawowych potrzeb człowieka jest potrzeba bezpieczeństwa. Dla jej zapewnienia powołuje się do życia wiele wyspecjalizowanych organizacji. Jedną z nich są Siły Zbrojne (wojsko). Ich funkcje i zadania dotyczą zapewnienia bezpieczeństwa w różnych wymiarach –również poprzez udział w misjach poza granicami kraju. Dlatego niezbędne jest dążenie do tego, aby wojsko było postrzegane przez społeczeństwo jako nowoczesna formacja, zdolna do reagowania nawet w najbardziej ekstremalnych sytuacjach. Dotyczy to zarówno samej struktury Sił Zbrojnych, jak i sposobów rozpowszechniania w społeczeństwie informacji na temat ich roli i oswajania społeczeństwa ze współczesnymi zagrożeniami.

Dokonując oceny z perspektywy czasu, jaki upłynął od momentu zaangażowania się Polski w operację iracką i afgańską, można uznać, że zaangażowanie wojskowe było pojmowane jako długoterminowa inwestycja w bezpieczeństwo Polski oraz budowanie bezpiecznej przyszłości. Były minister obrony narodowej Jerzy Szmajdziński podkreślał: „Taki jest żołnierski los, że trzeba być gotowym do działania nie tylko w granicach kraju, ale również daleko poza nimi dla światowego bezpieczeństwa. Bo światowe bezpieczeństwo to także bezpieczeństwo dla Polski. I często przeciwdziałanie niebezpieczeństwu w zarodku znacznie mniej kosztuje niż sytuacja, w której mamy do czynienia z bezpośrednim zagrożeniem".

Celem artykułu było scharakteryzowanie wybranych społecznych aspektów działań ekspedycyjnych prowadzonych przez Siły Zbrojne RP w ramach misji i operacji poza granicami kraju. Podsumowując, można zauważyć, że wszystkie społeczne aspekty udziału polskich żołnierzy w misjach i operacjach poza granicami przedstawione w tym artykule są bezpośrednio ze sobą powiązane. Dzięki kampaniom społecznym, działalności Centrum Weterana oraz akcjom mającym na celu udzielanie pomocy weteranom wzrasta pozytywne postrzeganie w społeczeństwie służby polskich weteranów, a także okazywanie im szacunku i wsparcia. To bardzo istotne, bo jeśli weterani cieszą się szacunkiem i wsparciem społeczeństwa, łatwiej im

powrócić do normalnego funkcjonowania w społeczeństwie i rodzinie. Z kolei jeśli społeczeństwo będzie popierać ekspedycyjną działalność Sił Zbrojnych, to żołnierze nadal będą służyć pod auspicjami ONZ, NATO czy UE.

Jako ostatni społeczny aspekt przedstawiono wpływ udziału w misjach i operacjach poza granicami kraju na przyspieszenie procesu profesjonalizacji i modernizacji technicznej polskiej armii. Wszystkie przedstawione aspekty oddziaływają na siebie, a nawet ze sobą korelują, a idące za tym społeczne konsekwencje, zarówno dla uczestników misji, jak i całego społeczeństwa polskiego, były widoczne w odniesieniu do udziału w dwóch szczególnych misjach – irackiej i afgańskiej.

Coraz powszechniej dostrzega się, że wojsko nie jest jednorodną grupą, ale że tworzą je ludzie o różnych systemach wartości, poziomie wiedzy i doświadczeń, pochodzący z różnych środowisk. Istotne staje się więc odpowiednie zarządzanie zasobami ludzkimi, ściślej: zarządzanie różnorodnością, aby wykorzystać indywidualne cechy i zaangażowanie żołnierzy do wzrostu efektywności zespołu (jednostki) [Urbaniak 2014, s. 66].

Reasumując rozważania przedstawione w artykule, należy pamiętać też o tym, aby składać hołd tym wszystkim, którzy w sprawie pokoju oddali życie, bo dzięki ich poświęceniu świat staje się bezpieczniejszy.

Bibliografia

Baranowska A. (2013), *Człowiek w instytucji totalnej. Społeczne aspekty służby polskich żołnierzy poza granicami kraju*, zakład wydawniczy „Nomos", Kraków.

Chodyński A. (2015), *Społeczna i ekologiczna odpowiedzialność organizacji a bezpieczeństwo*, „Bezpieczeństwo. Teoria i Praktyka", nr 1.

Jureńczyk Ł. (2011), *Użycie Polskiego Kontyngentu Wojskowego w misjach pokojowych i stabilizacyjnych w południowo – zachodniej Azji w pierwszej dekadzie XXI wieku. Od zaangażowania do wycofania*, „Rocznik Bezpieczeństwa Międzynarodowego", t. 5, Poznań.

Krzemińska A. (2016), *Społeczne aspekty udziału Sił Zbrojnych Rzeczypospolitej Polskiej w misjach i operacjach poza granicami kraju (część I)*, „Obronność, Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia AON", nr 1(17), Warszawa.

Paszkowski M. (2011), *Profesjonalizacja Sił Zbrojnych RP jako przykład zmian w wielkich grupach społecznych*, „Bezpieczeństwa Narodowe", nr 19, III.

Stachowicz-Stanusch A. (2007), *Potęga wartości. Jak zbudować nieśmiertelną firmę*, One Press, Helion, Gliwice.

Urbaniak B. (2014), *Zarządzanie różnorodnością zasobów ludzkich w organizacji*, „Zarządzanie Zasobami Ludzkimi", nr 3–4.

Wolin M. (2010), *Prasowcy PKW: Irak – Czad – Afganistan*, Wojskowe Centrum Edukacji Obywatelskiej.

Ustawa z dnia 19 sierpnia 2011 roku o weteranach działań poza granicami państwa [Dz. U. z 2011 r., poz. 1203].

Pamięci poległych w misjach poza granicami kraju [online], http://www.wojsko-polskie.pl/pl/pamieci-poleglych//, dostęp: 1.02.2018 r.

Udział Polski w operacji NATO w Afganistanie i jego konsekwencje BS/159/2010 [online], http://www.cbos.pl/SPISKOM.POL/2010/K_159_10.PDF/, dostęp: 1.03.2018 r.

Stosunek do obecności żołnierzy polskich w Iraku i Afganistanie BS/162/2007 [online], https://www.cbos.pl/SPISKOM.POL/2007/K_162_07.PDF/, dostęp: 1.03.2018 r.

Jerzy Telak | jtelak@spoleczna.pl
Społeczna Akademia Nauk, Wydział Nauk o Zarządzaniu i Bezpieczeństwie

Katarzyna Gad | katarzynag_1993@onet.pl

Prawo międzynarodowe jako narzędzie zwalczania handlu ludźmi

Wprowadzenie

Współcześnie handel ludźmi stał się poważnym przestępstwem naruszającym podstawowe prawa człowieka. Jest to zjawisko wieloczynnościowe, obejmujące szereg działań niezgodnych z obowiązującym kanonem prawnym, a ponadto jest trzecim pod względem wielkości dochodów nielegalnym interesem, zaraz po handlu bronią i narkotykami. Zgodnie z raportem Biura Narodów Zjednoczonych ds. Narkotyków i Przestępczości (United Nations Office on Drugs and Crime) [www.unodc.org/] handel ludźmi wytwarza roczny dochód oscylujący koło 32 miliardów dolarów [Biuro Narodów Zjednoczonych].

Handel ludźmi obejmuje: „werbowanie, transport, przekazywanie, przechowywanie lub przyjmowanie osób z zastosowaniem gróźb lub użyciem siły, lub też wykorzystaniem innej formy przymusu, uprowadzenia, oszustwa, wprowadzenia w błąd, nadużycia władzy lub wykorzystania słabości, wręczenia lub przyjęcia płatności lub korzyści dla uzyskania zgody osoby mającej kontrolę nad inną osobą, w celu wykorzystania" [Dz. U. z 2005 r. Nr 18, poz. 160, art. 3].

Zgoda osoby, która padła ofiarą handlu żywym towarem nie ma znaczenia w przypadku, gdy została względem niej zastosowana którakolwiek z metod wymienionych w definicji Protokołu dodatkowego o zapobieganiu, zwalczaniu oraz karaniu handlu ludźmi, w szczególności kobietami i dziećmi, uzupełniającym Konwencję Narodów Zjednoczonych o zorganizowanej przestępczości międzynarodowej z 2000 r. oraz Konwencji Rady Europy z 2005 r. Za handel ludźmi uznaje się także werbowanie, transport, przekazywanie, przechowywanie oraz przyjęcie dziecka celem

jego wykorzystania, nawet wtedy, gdy nie obejmuje żadnej z określonych w zapisie protokołu metod [Dz. U. z 2005 r. Nr 18, poz. 160, art. 3; Dz. U. z 2009 r. Nr 20, poz. 107].

Przestępstwo handlu ludźmi wiąże się z ruchami migracyjnymi, ma więc charakter ponadnarodowy. W dużej mierze wynika ono z występowania różnic oraz problemów natury ekonomicznej, społecznej i kulturowej. Można się zatem doszukiwać eskalacji handlu żywym towarem przede wszystkim w rejonach kryzysów politycznych, wojen, sporów militarnych oraz w przypadku krajów docelowych, w miejscach pozornej równowagi gospodarczej. Z uwagi na skalę problemu organizacje narodowe i międzynarodowe pracują nad tworzeniem instrumentów, które mają zapobiegać pojawianiu się niepożądanego procederu, a w przypadku jego zaistnienia – zastosowania nowoczesnych metod zmierzających do zniwelowania zjawiska.

Dla potrzeb niniejszego artykułu postawiono za cel badawczy identyfikację międzynarodowych przepisów prawnych dotyczących zwalczania handlu ludźmi oraz wskazanie możliwości doskonalenia narzędzi i rozszerzenia zakresu przeciwdziałania tej przestępczości. Przy tym celu sformułowano problemy badawcze zawarte w pytaniach:

- jakie międzynarodowe narzędzia prawne wykorzystuje się do zwalczania handlu ludźmi?
- jak doskonalić narzędzia prawne i rozszerzyć zakres przeciwdziałania, aby wzrosła efektywność zwalczania handlu ludźmi?

Narzędzia przeciwdziałania handlowi ludźmi w prawie międzynarodowym

Z uwagi na duże zainteresowanie wynikające z powszechności zjawiska handlu ludźmi, sposoby jego zwalczania znalazły wyraz w wielu aktach prawa międzynarodowego [por. Morawska 2006, s. 57]. Powszechną organizacją prawną odnoszącą się do przeciwdziałania handlowi ludźmi jest Organizacja Narodów Zjednoczonych (*United Nations*, ONZ) [www.un.org/en/; https://www.msz.gov.pl/pl/polityka_zagraniczna/organizacje_miedzynarodowe/organizacja_narodow_zjednoczonych]. Działanie ONZ opiera się na trzech aktach prawa międzynarodowego:

- Karcie Narodów Zjednoczonych [Dz. U. z 1947 r. Nr 23, poz. 90; Dz. U. z 1946 r. Nr 2, poz. 6; Dz. U. z 1947 r. Nr 23, poz. 91],
- Powszechnej Deklaracji Praw Człowieka (Universal Declaration of Human Rights) [Rez. Z.O. ONZ 217 A (III) 1948], Ustawie z dnia 17 maja 1989 r. o gwarancjach wolności sumienia i wyznania [t.j. Dz. U. z 2017 r., poz. 1153],

- Międzynarodowych Paktów Praw Człowieka [Dz. U. z 1977 r. Nr 38, poz. 167].

Pierwszy o szerokim wymiarze dokument dotyczący zwalczania handlu ludźmi stanowi Międzynarodowe porozumienie w sprawie zwalczania handlu ludźmi białymi niewolnikami z 1904 r. Głównym celem tego porozumienia było zapewnienie ochrony dziewczynkom i kobietom przed przymusowym procederem nierządu, które określono jako: „handel białymi". W nawiązaniu do działań związanych z wykorzystaniem podstępu bądź przymusu do werbowania osób w celu nierządu, w 1910 r. została podpisana Międzynarodowa konwencja o zwalczaniu handlu białymi niewolnikami, w której po raz pierwszy handel ludźmi otrzymał miano przestępstwa [Dz. U. z 1952 r. Nr 13, poz. 78].

Liga Narodów w 1921 r. uchwaliła Konwencję o zwalczaniu handlu kobietami i dziećmi, która, oprócz tego, że stanowiła dopełnienie poprzednich konwencji, została rozbudowana o problematykę uczestnictwa chłopców w procederze handlu ludźmi. Dodatkowo została również podniesiona granica wieku małoletnich z 20 na 21 lat [Dz. U. z 1925 r. Nr 125, poz. 893].

W 1926 r. w Konwencji w sprawie niewolnictwa zawarto definicję handlu niewolnikami oraz prawny nakaz zlikwidowania wszelakich czynności, które przybierały formę niewolnictwa [Dz. U. z 1931 r. Nr 4, poz. 21]. Konwencja o zwalczaniu handlu kobietami pełnoletnimi z 1933 r. nakazywała: „poddanie karze każdego, kto dla zaspokojenia namiętności innych osób werbuje, uprowadza lub uwodzi kobietę lub dziewczynę pełnoletnią, nawet za jej zgodą, mając przy tym na celu przeznaczenie jej do prowadzenia nierządu w innych krajach, choćby nawet poszczególne działania, należące do istoty przestępstwa, popełnione były w różnych krajach" [Dz. U. z 5 lutego 1938 r.; Dz. U. z 1937 r. Nr 25, poz. 164].

Po zakończeniu II wojny światowej, w Lake Success, 21 marca 1950 r. została podpisana Konwencja w sprawie zwalczania handlu ludźmi i eksploatacji prostytucji, która skonsolidowała postanowienia wszystkich poprzednich konwencji międzynarodowych, a następnie ratyfikowana w 1952 r. [Dz. U. z 1952 r. Nr 41, poz. 278]. Zgodnie z art. 1 tej konwencji, surowe restrykcje dotyczyły karania każdego „kto zmusza, doprowadza podstępem bądź dostarcza osobę do wykorzystania jej w celach prostytucji, bądź nawet za zgodą osoby prostytucję uprawia". Ponadto problem nierządu powiązano z migracją, co w rezultacie przyczyniło się do nałożenia na państwa obowiązku kontroli ruchów migracyjnych. Znaczącym uchybieniem był brak sprecyzowania zasad kontroli i jej form [Dz. U. z 1952 r. Nr 13, poz. 78].

Na początku XXI w. Zgromadzenie Ogólne ONZ przyjęło Konwencję Narodów przeciwko międzynarodowej przestępczości zorganizowanej w celu zahamowania rozprzestrzeniania się działalności zorganizowanych grup przestępczych, co

w rezultacie doprowadziło również do zakwalifikowania handlu ludźmi jako formy międzynarodowej przestępczości zorganizowanej. Następstwem nasilenia nielegalnej działalności zorganizowanej na skalę międzynarodową była niemożność zapewnienia wystarczającej ochrony potencjalnym ofiarom handlu ludźmi oraz odbicia osób już uprowadzonych z rąk przestępców. Nowa regulacja objęła sprawy prewencji, zapobiegania, ścigania i karania wszystkich form przestępczości zorganizowanej [Dz. U. z 2005 r. Nr 18, poz. 158].

We współpracy policyjnej w sferze międzynarodowej pierwszoplanową rolę odgrywa Międzynarodowa Organizacja Policji (*International Criminal Police Organization*, Interpol) [https://www.interpol.int/]. Celem działalności Interpolu jest doskonalenie i zacieśnianie współpracy pomiędzy jednostkami policyjnymi państw świata w celu szybszego przekazu informacji, a co za tym idzie szybszego przechwytywania sprawców przestępstw. Swoją strategię działania Interpol opracowuje na nowo co 3 lata, w celu pełnego wykorzystania sił i środków policyjnych. W związku z rozprzestrzeniającym się zjawiskiem handlu ludźmi Interpol doskonali rozwiązania taktyczne. Priorytet stanowi międzynarodowa wymiana informacji pomiędzy jednostkami policyjnymi o osobach ściganych i potencjalnych ofiarach, pomoc w śledztwach i dochodzeniach oraz koordynowanie działań państw w zakresie przeciwdziałania i walki z rozprzestrzeniającą się przestępczością zorganizowaną [Sońta 2015, ss. 89–96].

W ramach swojej działalności Interpol zajmuje się również prowadzeniem czynności mających na celu likwidację konkretnych obszarów form przestępczości zorganizowanej bądź przynajmniej zmniejszeniem skali problemu. Jedna z przeprowadzonych akcji (o nazwie TUY) odbicia z rąk handlarzy dzieci zmuszanych do pracy na terenie Burkina Faso zakończyła się sukcesem. W przeciągu dwóch dni, funkcjonariuszom udało się uratować około 400 dzieci. Oprócz spraw związanych z przymusową pracą, Interpol prowadzi również walkę z prostytucją i pornografią. Dzięki bazie danych i dostępowi do informacji zgromadzonych w różnych państwach, Interpol prowadzi działania na całym świecie, skutecznie zwalczając przejawy handlu ludźmi i przestępczości zorganizowanej [Sońta 2015, s. 92].

Organizacja Paktu Północnoatlantyckiego (NATO) również zajmuje się walką z handlem ludźmi. Sprecyzowanie działań nastąpiło na Szczycie NATO w Stambule w kwietniu 2004 r., podczas którego przyjęto tzw. Politykę NATO przeciwko handlowi ludźmi. Określiła ona handel żywym towarem jako jedną z najsurowszych zbrodni, stanowiącą dodatkowo element przestępczości zorganizowanej. Celem polityki NATO jest wyeliminowanie wszystkich form handlu ludźmi, przede wszystkim handlu dziećmi i kobietami. Aby działania były skuteczniejsze, NATO

prowadzi szkolenia dla personelu, uczestniczy w misjach pokojowych oraz podpisuje kontrakty, które uniemożliwiają osobom podpisującym je prowadzenie działań związanych z handlem ludźmi [Sońta 2015, ss. 89–96].

Narzędzia przeciwdziałania handlowi ludźmi w prawie europejskim

Z uwagi na związek z prawami człowieka, handel ludźmi znalazł się również w kręgu zainteresowania Organizacji Bezpieczeństwa i Współpracy w Europie – OBWE (*Organization for Security and Co-operation in Europe*, OSCE) [https://www.osce.org/; https://www.msz.gov.pl/pl/polityka_zagraniczna/europa/obwe/], która skupia się na:

- wywieraniu wpływu na świadomość rządów państw członkowskich;
- prowadzeniu szkoleń dla funkcjonariuszy Policji i Straży Granicznej dotyczących rozpoznawania działań o znamionach handlu żywym towarem;
- zapewnianiu bezpiecznych schronień dla osób poszkodowanych;
- przygotowywaniu projektów aktów prawnych niezbędnych w procesie sądzenia sprawców [Pawłowski 2014, ss. 40–43].

Kolejną europejską organizacją zajmującą się zwalczaniem handlem ludźmi jest Unia Europejska (*European Union*, UE). 29 listopada 1996 r. Rada UE przyjęła wspólne działanie 96/700/WSiSW w sprawie powołania programu STOP przeciwko handlowi ludźmi i seksualnemu wykorzystywaniu dzieci, które obowiązywało w ramach trzeciego filaru UE w latach 1993–1999 [Dz. Urz. WE L 63 z 4 marca 1997 r., s. 2]. Program ten dotyczył przeciwdziałania handlowi żywym towarem i seksualnemu wykorzystaniu dzieci. Priorytetowym celem, prócz zwalczania form handlu ludźmi, była także walka z nielegalną migracją, a także polepszenie międzynarodowej współpracy sądowej. Zgodnie z wytycznymi dokumentu, jako handel ludźmi określano: „jakiekolwiek postępowanie ułatwiające wjazd, tranzyt, pobyt lub wyjazd z terytorium Państwa, natomiast wykorzystywanie seksualne oznacza nakłanianie lub zmuszanie do jakiejkolwiek czynności seksualnej, oraz wykorzystanie do prostytucji lub innych nielegalnych praktyk seksualnych" Programy STOP zostały z czasem zastąpione przez programy Daphne, Daphne II i Daphne III, skupiające się na walce z przemocą wobec kobiet oraz walce z handlem ludźmi [Sońta 2015, ss. 78–80].

UE nałożyła na państwa członkowskie obowiązek podejmowania odpowiednich środków w celu zapobiegania i przeciwdziałania handlowi ludźmi. Ważną rolę w tym odgrywa kontrola graniczna, podczas której w razie wykrycia przestępstwa

należy skonfiskować narzędzia zbrodni, przejąć ofiarę i w miarę możliwości środki pieniężne. Następnie należy poinformować odpowiednie służby, a do czasu ich przybycia zatrzymać sprawcę z jednoczesnym poszanowaniem praw do prywatności osobistej. Państwa członkowskie zobligowano do zapewnienia pomocy ofiarom i członkom rodziny, a także do współpracy sądowniczej w ramach prowadzonych postępowań i spraw sądowych [Sońta 2015, ss. 80–84]. Rezolucja Parlamentu Europejskiego w sprawie eliminacji przemocy wobec kobiet [Dz. Urz. WE 2010/C 285 E/07] oraz Konwencja Rady Europy o zapobieganiu i zwalczaniu przemocy wobec kobiet i przemocy domowej [Dz. U. z 2015 r., poz. 961; CETS nr 5, 1950; CETS nr 35, 1961; CETS nr 163, 1996; CETS nr 197, 2005; CETS nr 201, 2007] stanowią dopełnienie prawa UE.

Oprócz działań legislacyjnych, UE bierze także udział w działaniach koordynacyjnych i politycznych. Na początku XXI w. zostało utworzone europejskie forum ds. walki z przestępczością zorganizowaną, podczas którego poruszano tematy dotyczące problematyki handlu ludźmi [Sońta 2015, ss. 80–82].

W związku z współzależnością pomiędzy handlem ludźmi a przestępczością zorganizowaną, Komisja Europejska przyjęła Plan Działań, którego następstwem ma być zmniejszenie do minimum omawianej formy przestępczości zorganizowanej. Plan Działań obejmuje przede wszystkim równość płci, politykę społeczną i politykę sąsiedztwa oraz kwestię migracji. Dodatkowo ważnym elementem planu jest próba większego zaangażowania Europejskiego Urzędu Policji (*European Police Office*, Europol) w prowadzone działania [Sońta 2015, ss. 82–84].

Do zadań Europolu [https://europa.eu/european-union/content/european-police-officeeuropol_pl] należy organizowanie wymiany informacji pomiędzy państwami członkowskimi, prowadzenie analiz operacyjnych oraz tworzenie baz danych o sprawcach przestępstw i ich ofiarach. Narzędziem wykonawczym Europolu są oficerowie łącznikowi, którzy należą do różnych jednostek sił policyjnych. Dla Europejskiego Biura Policji została utworzona osobna definicja handlu ludźmi w celu wykorzystywania seksualnego, według której handel ludźmi określa się jako: „oddanie rzeczywistej i niezgodnej z prawem władzy innych osób przy użyciu przemocy i groźby lub przez nadużycie władzy albo podstęp w celu eksploatacji prostytucji i innej formy eksploatacji seksualnej i wykorzystania nieletnich lub handel porzuconymi dziećmi" [Rau 2002, s. 90].

Przykładem działania Europolu w sferze zwalczania handlu ludźmi była akcja SAMOT przeciwko Irakijczykom zajmującym się nielegalnym przemytem ofiar, w głównej mierze do państw skandynawskich, a także Wielkiej Brytanii i Kanady [www.europol.europa.eu/index.asp?/page=publar1999#OPERATION%20SAMOT].

Kolejną wielką akcją zakończoną sukcesem była operacja GIRASOLE (słonecznik). Działaczom Europolu udało się zlikwidować liczne drogi transportujące ofiary handlu ludźmi na obszarze całej Europy. Po tej operacji podjęto także działania dążące do poprawy współpracy instytucji oraz organizacji rządowych wielu europejskich państw [Letkiewicz 2010, s. 12].

Ochrona ofiar handlu ludźmi w ustawodawstwie międzynarodowym

W celu zakwalifikowania kogoś jako ofiary handlu ludźmi, na początek należy zidentyfikować osobę. Często poszkodowani sami nie zdają sobie sprawy z zaistniałego wydarzenia i nie utożsamiają się z osobą pokrzywdzoną. Czynnikami, które zakłócają odpowiednio szybką identyfikację ofiar, są przede wszystkim traumatyczne przeżycia, brak zaufania do służb bezpieczeństwa i służb porządkowych oraz organów wymiaru sprawiedliwości, bariery językowe bądź kulturalne, a także strach przed zemstą ze strony sprawców [Pawłowski 2014, ss. 76–88].

Ważną rolę w procesie identyfikacji odgrywają: Policja, Straż Graniczna, służby imigracyjne i pracownicy służby zdrowia. Służby te najczęściej jako pierwsze mają kontakt z ofiarą. To w dużej mierze od ich doświadczenia oraz podejścia zależy otwarcie się osoby poszkodowanej oraz jej chęć rozmowy o swoich przeżyciach i szukanie pomocy. W związku z tym funkcjonariusze i pracownicy służb mających możliwość spotkania się z osobami dotkniętymi przemocą powinni rozumieć znaczenie takich czynników jak: płeć, wiek, kontekst religijny, kulturowy oraz obawa przed zemstą i prześladowaniem [Pawłowski 2014, ss. 76–88].

W wielu przypadkach, dodatkowym problemem w zidentyfikowaniu ofiary jest wstępne zakwalifikowanie jej jako sprawcy czynu zabronionego, a nie postrzeganie jako osoby poszkodowanej. Rozpoznanie osób jako pokrzywdzonych przyczynia się do zwolnienia ich z odpowiedzialności za popełnione czyny, które w świetle prawa spełniają znamiona przestępstwa. Do czynów zabronionych należą m. in. posługiwanie się fałszywymi dokumentami lub nielegalne przekroczenie granicy. Pomimo faktu zaistnienia czynu zabronionego, osoby, które go popełniły nie dokonały go z własnej woli, w związku z czym są one ofiarą, nie sprawcą. Wyróżnia się dwa schematy niekarania ofiar. Pierwszy to schemat przyczynowy, który nakazuje zaniechanie ścigania czynów niezgodnych z prawem związanych z procederem handlu ludźmi, drugi to model przymusowy, który wyłącza ściganie osoby zmuszonej do popełnienia przestępstwa [Pawłowski 2014, ss. 82–84].

Problematyka ochrony ofiar handlu ludźmi po raz pierwszy została poruszona w Protokole w sprawie handlu dziećmi. Zgodnie z jej zapisem: „Państwa mają podejmować odpowiednie kroki w celu ochrony praw i interesów dzieci ofiar handlu na wszystkich etapach postępowania karego, w szczególności poprzez właściwą ochronę interesów prywatności i tożsamości dzieci ofiar oraz podjęcie środków, zgodnych z prawem krajowym, w celu uniknięcia niewłaściwego rozpowszechnienia informacji mogących doprowadzić do identyfikacji dzieci ofiar" [Dz. U. z 2007 r. Nr 76, poz. 494, art. 8 ust. 1 pkt e].

Zagadnienie ochrony ofiar handlu żywym towarem znalazło miejsce w Konwencji warszawskiej. Każde państwo ma obowiązek zapewnić ochronę osobie będącej ofiarą handlu ludźmi. Co więcej, tożsamość i szczegóły naruszenia prawa nie mogą być podane do wiadomości publicznej. Wyjątek stanowi sytuacja, w której ujawienie tożsamości ofiary pomoże w jej odnalezieniu lub identyfikacji. Zapewnia się również ochronę tożsamości w postępowaniu sądowym, poprzez wyłączenie z części bądź z całej rozprawy mediów i publiczności czy też przez możliwość potraktowania ofiary jako tzw. świadka anonimowego [Dz. U. z 2007 r. Nr 76, poz. 494, art. 11].

Osoby będące ofiarami handlu ludźmi powinny mieć zapewniony dostęp do pomocy medycznej, socjalnej, prawnej oraz psychologicznej. Aby powrót do normalnego życia mógł nastąpić sprawnie, ważne jest wzajemne powiązanie pomiędzy każdą z form udzielanego wsparcia. Rodzaj odpowiedniego zakwaterowania powinien być związany z warunkami osobistymi ofiary, a mianowicie nie powinno się umieszczać ofiar handlu ludźmi w ośrodkach dla cudzoziemców bądź w aresztach, gdzie mogą się spotkać z przemocą i agresją [Pawłowski 2014, ss. 82–88].

Pomoc medyczna w pierwszej kolejności powinna być udzielana osobom bitym bądź eksploatowanym. Taka forma ratunku może również pomóc w zabezpieczeniu dowodów, w celu ich późniejszego wykorzystania w postępowaniu przeciwko sprawcom. Dodatkowo w przypadku ofiar gwałtów i osób zmuszanych do prostytucji, badania lekarskie umożliwią identyfikacje obecności wirusa HIV, a im szybciej nastąpi, tym będzie miało to mniej poważne skutki dla osoby poszkodowanej. W przypadku ofiary z innego państwa, niezmiernie ważne jest zagwarantowanie kontaktu z tłumaczem, najlepiej z rodzimego kraju poszkodowanego. Przyczyni się to do zniwelowania bariery językowej i umożliwi ofierze dochodzenie swoich praw [Pawłowski 2014, ss. 82–88].

Konwencja z Lake Success w kontekście handlu ludźmi stwierdza, że państwa powinny zachęcać osoby pokrzywdzone do podjęcia działań umożliwiających pomoc w zlikwidowaniu bądź przynajmniej w pewnym stopniu zmniejszeniu

traumatycznych przeżyć. Umożliwienie tego następuje poprzez udostępnianie przez państwa placówek zdrowotnych, oświaty, społecznych czy gospodarczych. Udzielenie ofiarom wsparcia znacznie zwiększa prawdopodobieństwo podjęcia przez nie współpracy z wymiarem sprawiedliwości, co z kolei wiąże się z możliwością wykrycia sprawców i zapobieżeniem dalszego popełniania przestępstw [Pawłowski 2014, ss. 82–88].

Podsumowanie

Zjawisko handlu ludźmi jest niezwykle poważnym problemem XXI wieku. Tylko w Polsce, gdzie jesteśmy przede wszystkim krajem tranzytowym, według statystyk rocznie ofiarami handlu żywym towarem pada około 200 osób. W statystyce tej warto wziąć pod uwagę tzw. ciemną liczbę przestępstw, wynikającą przede wszystkim ze strachu przed oprawcą bądź chęcią jak najszybszego wymazania z pamięci zaistniałych traumatycznych zdarzeń. Szacunkowo rocznie około 15 tys. Polaków staje się ofiarą przestępstwa handlu ludźmi. Dzięki współpracy międzynarodowej, rezultaty walki z procederem handlu ludźmi mają szansę na osiągnięcie wyższego poziomu na korzyść organizacji oraz państw zmagających się z omawianym zjawiskiem. Aby działania te były skuteczniejsze potrzeba szeregu przedsięwzięć.

Wnioski

1. Wyroki skazujące za handel ludźmi należy orzekać proporcjonalnie do wagi popełnionego bezprawnie czynu.
2. Należy usprawnić centralną koordynację działań oraz gromadzić i przetwarzać aktualne dane statystyczne na temat zmagań z handlem ludźmi.
3. Prokuratorów i sędziów oraz funkcjonariuszy i pracowników służb mających styczność z handlem ludźmi należy szkolić w zakresie przepisów i taktyki postępowania z ofiarami.
4. Należy powoływać wyspecjalizowane jednostki prokuratury zajmujące się problematyką handlu ludźmi.
5. Działania w zakresie identyfikacji ofiar należy wzmóc przede wszystkim wśród dzieci i młodzieży.

Bibliografia

Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (GLOTIP) (2016), *Światowy raport nt. Handlu ludźmi 2016*, grudzień 2016 r. [online], https://handelludzmi.eu/hl/baza-wiedzy/raporty-analizy-strateg/raporty-dotyczace-sytua/6898,Raport-UNODC-GLOTIP-2016.html, dostęp: 18.10.2018.

Europejska karta społeczna (CETS nr 35, 1961, zmieniona w 1996, CETS nr 163).

https://europa.eu/european-union/content/european-police-officeeuropol_pl, dostęp: 12.10.2018.

https://www.interpol.int/, dostęp: 18.10.2018.

https://www.msz.gov.pl/pl/polityka_zagraniczna/europa/obwe/, dostęp: 12.10.2018.

https://www.msz.gov.pl/pl/polityka_zagraniczna/organizacje_miedzynarodowe/organizacja_narodow_zjednoczonych/, dostęp: 18.10.2018.

https://www.osce.org/, dostęp: 12.10.2018.

Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych (Dz. U. z 1947 r. Nr 23, poz. 90).

Konwencja międzynarodowa z dnia 11 października 1933 r. o zwalczaniu handlu kobietami pełnoletnimi (Dz. U. z 5 lutego 1938 r.).

Konwencja międzynarodowa z dnia 30 września 1921 r. o zwalczaniu handlu kobietami i dziećmi (Dz. U. z 1925 r. Nr 125, poz. 893).

Konwencja Narodów przeciwko międzynarodowej przestępczości zorganizowanej, 15.11.2000 r. (Dz. U. z 2005 r. Nr 18, poz. 158).

Konwencja o ochronie praw człowieka i podstawowych wolności (CETS nr 5, 1950).

Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych (CETS nr 201, 2007).

Konwencja Rady Europy o zapobieganiu i zwalczaniu przemocy wobec kobiet i przemocy domowej, sporządzona w Stambule dnia 11 maja 2011 r. (Dz. U. z 2015 r., poz. 961).

Konwencja Rady Europy w sprawie działań przeciwko handlowi ludźmi, sporządzona w Warszawie dnia 16 maja 2005 r. (Dz. U. z 2009 r. Nr 20, poz. 107).

Konwencja Rady Europy w sprawie działań przeciwko handlowi ludźmi (CETS nr 197, 2005).

Konwencja w sprawie niewolnictwa, podpisana w Genewie dnia 25 września 1926 r. (Dz. U. z 1931 r. Nr 4, poz. 21).

Konwencja z dnia 21 marca 1950 r. w sprawie zwalczania handlu ludźmi i eksploatacji prostytucji (ratyfikowana na podstawie ustawy z dnia 29 lutego 1952 r.) (Dz. U. z 1952 r. Nr 41, poz. 278).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167).

Letkiewicz A. (2010), *Rola Europolu w systemie bezpieczeństwa Unii Europejskiej*, „Zeszyt naukowy" nr 1, wyd. Powszechna Wyższa Szkoła Humanitarna, Chojnice, ss. 11-21.

Morawska E. (2006), Handel ludźmi z perspektywy systemu ochrony praw człowieka ONZ [w:] Z. Lasocik red., *Handel ludźmi. Zapobieganie i ściganie*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa.

Operacja SAMOT [online], www.europol.europa.eu/index.asp?/page=publar1999#OPERATION%20SAMOT, dostęp: 25.09.2018.

Oświadczenie Rządowe z dnia 8 lipca 1946 r. w sprawie ratyfikacji przez Polskę Karty Narodów Zjednoczonych podpisanej w Waszyngtonie dnia 16 października 1945 r. (Dz. U. z 1947 r. Nr 23, poz. 91).

Pawłowski M. (2014), *Międzynarodowe standardy ścigania handlu ludźmi i ochrony jego ofiar*, wyd. Helsińska Fundacja Praw Człowieka, Warszawa.

Powszechna Deklaracja Praw Człowieka z 1948 r. (Rez. Z.O. ONZ 217 A (III), 10 grudnia 1948 r.).

Protokół Fakultatywny do Konwencji o prawach dziecka w sprawie handlu dziećmi, dziecięcej prostytucji i dziecięcej pornografii (Dz. U. z 2007 r. Nr 76, poz. 494).

Protokół o zapobieganiu, zwalczaniu oraz karaniu za handel ludźmi, w szczególności kobietami i dziećmi, uzupełniający Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej, przyjęty przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r. (Dz. U. z 2005 r. Nr 18, poz. 160).

Rau Z. (2002), *Przestępczość zorganizowana w Polsce i jej zwalczanie*, Kantor Wydawniczy Zakamycze, Kraków.

Rezolucja Parlamentu Europejskiego z dnia 26 listopada 2009 r. w sprawie eliminacji przemocy wobec kobiet P7_TA (2009)0098 (Dz. Urz. WE 2010/C 285 E/07).

Sońta K. (2015), *Przeciwdziałanie handlowi ludźmi w prawie międzynarodowym*, praca doktorska, UW, Wydział Prawa i Administracji, Warszawa.

Stanowisko Rady Unii Europejskiej 97/154/WSiSW dotyczące zwalczania handlu ludźmi i seksualnego wykorzystywania dzieci (Dz. Urz. WE L 63 z 4 marca 1997 r.).

Ustawa z dnia 17 maja 1989 r. o gwarancjach wolności sumienia i wyznania (Dz. U. z 1989 r. Nr 29, poz. 155, t.j. Dz. U. z 2017 r., poz. 1153).

Ustawa z dnia 18 marca 1937 r. o ratyfikacji konwencji międzynarodowej, dotyczącej zwalczania handlu kobietami pełnoletnimi, podpisanej w Genewie dnia 11 października 1933 r. (Dz. U. z 1937 r. Nr 25, poz. 164)

Ustawa z dnia 29 lutego 1952 r. w sprawie zwalczania handlu ludźmi i eksploatacji prostytucji (Dz. U. z 1952 r. Nr 13, poz. 78).

Ustawa z dnia 31 grudnia 1945 r. o ratyfikacji podpisanych w San Francisco dnia 26 czerwca 1945 r. Karty Narodów Zjednoczonych oraz Porozumienia ustanawiającego Komisję Przygotowawczą Narodów Zjednoczonych (Dz. U. z 1946 r. Nr 2, poz. 6).

www.un.org/en/, dostęp: 18.10.2018.

www.unodc.org/, dostęp: 18.12.2018.

Piotr Rozwadowski | piotr_rozwadowski@o2.pl
Społeczna Akademia Nauk

Identyfikowanie wyzwań i sposoby rozwiązywania problemów bezpieczeństwa na szczeblu centralnym i stanowym w Indiach

Wstęp

Celem badań prowadzonych przez autora od 2015 r. jest ustalenie, w jaki sposób w jednym z najludniejszych i najszybciej rozwijających się państw świata wraz z postępem gospodarczo-społecznym zmieniają się wyzwania i szanse w dziedzinie bezpieczeństwa, a wraz z tym ewoluują świadomość społeczna, postawa władz oraz instytucje odpowiedzialne za ład, porządek i nienaruszalność granic Indii.

Dynamika rozwoju i zmian społecznych w Indiach nie spowolniła, wręcz przeciwnie, można zaobserwować jej wyraźne przyspieszenie w 2018 i 2019 r., co utrudnia całościowe uchwycenie opisywanych zjawisk. Poza tym współczesną literaturę poświęconą problematyce bezpieczeństwa wewnętrznego Indii należy ocenić jako niezwykle ubogą.

Pozyskanie pełnych i wiarygodnych danych dotyczących bezpieczeństwa, zwłaszcza wewnętrznego, w Indiach napotyka na istotne bariery. Sfera ta jest traktowana przez władze, zarówno centralne, jak i lokalne, jako niezwykle wrażliwa. Co za tym idzie, mieszkańcy Indii podchodzą do badań prowadzonych przez obcych naukowców z dużą rezerwą. Zarówno w trakcie prowadzenia wywiadów, jak i sondażu diagnostycznego metodą ankiety stanowczo zastrzegają sobie anonimowość. Ważnym źródłem informacji dla autora pozostają media, zwłaszcza prasa, telewizja i Internet. Niebagatelne znaczenia mają „ukryte" wywiady z miejscową ludnością, które w istocie polegają na poznawaniu opinii w trakcie rozmów z mieszkańcami kraju na bieżące tematy.

Dane do przeprowadzenia analizy pozyskiwane były przez autora w czasie licznych podróży do Indii i pobytu w takich ośrodkach, jak New Delhi, Mumbai, Chandigaru Czandigar, Bangalur.

Powyższe działania służyć miały weryfikacji postawionej przez autora hipotezy badawczej, iż system bezpieczeństwa narodowego Indii, zwłaszcza w sferze bezpieczeństwa wewnętrznego, ewoluuje wraz z postępem gospodarczo-społecznym tego kraju.

Uwarunkowania społeczno-polityczne bezpieczeństwa wewnętrznego współczesnych Indii

Dla współczesnych nauk społecznych Indie, dzięki dynamice przemian i rozwoju, są tym, czym dla badań w zakresie fizyki „wielki zderzacz hadronów". Współczesne Indie liczą 600 mln ludzi młodych, są największą demokracją liberalną świata, a jednocześnie 700 mln mieszkańców tego kraju nigdy nie korzystało z komputera. Dane encyklopedyczne dotyczące kraju przedstawiają się następująco: powierzchnia całkowita (7. miejsce na świecie) wynosi 3 287 590 km^2, wody śródlądowe – 314 400 km (9,56%), całkowita liczba ludności (2017) – 1 316 896 000, gęstość zaludnienia (2. miejsce na świecie) – 390 osób/km^2, PKB (2017) całkowite – 2611 mld USD, na osobę – 1983 USD (2017). Tempo wzrostu gospodarczego wynosi średnio ok. 8%

Jak podaje na swoich stronach internetowych Ministerstwo Spraw Zagranicznych Rzeczypospolitej Polskiej: „Indie są państwem demokratycznym o republikańskiej formie rządów, opartej na systemie westminsterskim. Konstytucja Indii została uchwalona 26 listopada 1949 r., weszła w życie, tj. 26 stycznia 1950 roku.

Indie są państwem federacyjnym z silną władzą centralną. Konstytucja wyraźnie rozgranicza kompetencje władz centralnych i lokalnych. Składają się z 28 stanów i 7 terytoriów (administracja wykonywana jest w nich bezpośrednio przez urzędników mianowanych i odwoływanych przez Prezydenta Indii).

Zgodnie z literą konstytucji, Indie są państwem świeckim, które gwarantuje podstawowe prawa człowieka: «sprawiedliwość (społeczną, ekonomiczną i polityczną), wolność (myśli, wypowiedzi, wierzeń, wiary i czci), równość (statusu i możliwości)». Wyżej wymienione zasady nie zawsze są implementowane wobec głęboko zakorzenionych zwyczajów, wierzeń i praktyk społecznych.

Konstytucja zakłada podział na władzę: wykonawczą (prezydent i rząd, rządy stanowe), ustawodawczą (dwuizbowy parlament Indii, legislatury stanowe) oraz

sądowniczą" [www.msz.gov.pl/pl/p/newdelhi_in_a_pl/wspolpraca_dwustronna/gospodarka_indii/ind_informacje/].

Kraj ten uczestniczy w jednym z najważniejszych konfliktów we współczesnym świecie, który nie został zakończony regulującymi go trwałymi traktatami pokojowymi, a mianowicie w trwającym od 1947 r. konflikcie indyjsko-pakistańskim. Przerodził się on w wojny w latach 1947–1948, 1965 (wojny o Kaszmir) i 1971. W wyniku tej ostatniej powstał Bangladesz. Bezpośrednią przyczyną konfliktu jest podział terenowo dawnych Indii Brytyjskich według kryteriów religijno-kulturowych na część hinduską (Indie) i muzułmańską – Pakistan[1].

Pierwsza wojna doprowadziła do wytyczenia linii zawieszenia broni, która z niewielkimi zmianami obowiązuje do czasów współczesnych. Po stronie indyjskiej pozostało około 73% powierzchni terytorium Kaszmiru i Dżammu, Lakdah i połowa Pańcz, po stronie pakistańskiej znalazły się: Gilgit, Baltisan, niewielki pas Kaszmiru, połowa Pańcz i część Dżammu.

Rada Bezpieczeństwa w jednej ze swych rezolucji podjęła decyzję o utworzeniu Komisji Narodów Zjednoczonych do spraw Indii i Pakistanu (United Nations Commission for India and Pakistan, UNCIP). Jednym z proponowanych rozwiązań było przeprowadzenie plebiscytu, do którego jednak nigdy nie doszło. Kolejna rezolucja, ze stycznia 1949 r., powołała Grupę Obserwatorów Wojskowych Narodów Zjednoczonych w Indiach i Pakistanie (United Nations Military Observer Group in India and Pakistan, UNMOGIP), która wytyczyła linię wstrzymania ognia.

W latach sześćdziesiątych XX w. do konfliktu włączyły się Chiny (ChRL), które zawarły sojusz z Pakistanem i w zmian za skrawek terytorium zagwarantowały wspólną granicę. Następnie zaatakowały Indie i odebrały im obszar Aksai Chin. Indie uzyskały wsparcie państw Zachodu, co doprowadziło do szybkiego zakończenia konfliktu granicznego. Druga wojna indyjsko-pakistańska miała miejsce w sierpniu 1965 r. Wśród przyczyn sporu wymienić należy aresztowanie przywódcy ludności muzułmańskiej w Indiach szejka Abdullaha oraz protesty islamistów w przygranicznych miejscowościach, które doprowadziły do ataku islamskich ekstremistów i przekroczenia przez nich linii zawieszenia broni. Spotkało się to z szybką odpowiedzią armii indyjskiej. 1 września Pakistan wypowiedział Indiom wojnę i przeszedł do regularnych działań zbrojnych. Uzyskał wsparcie innych państw muzułmańskich: z Indonezji przybyli ochotnicy, a Turcja i Iran dostarczyły broni i amunicji. Wojna zakończyła się 23 września 1965 r. po zaakceptowaniu przez obie strony wezwania RB ONZ do zawieszenia broni. 4 stycznia 1966 r. w Taszkiencie

[1] Opis konfliktu za: [www.prezi.com/lgmi5rm7igih/konflikt-indyjsko-pakistanski/] oraz [Dobrzelewski 2016].

w ZSRR rozpoczęły się rozmowy premiera Indii Lal Bahadura Shastriego i prezydenta Pakistanu Ayub Khana. Dzięki mediacji premiera ZSRR Aleksieja Kosygina 10 stycznia 1966 r. podpisana została 9-punktowa deklaracja taszkiencka przewidująca normalizację stosunków dwustronnych, pokojowe rozwiązywanie sporów i wycofanie wojsk na pozycje sprzed drugiej wojny 1965 r. [Dobrzelewski 2016].

Trzecia wojna pakistańsko-indyjska

Trzecia wojna stanowiła skutek polityki wewnętrznej Pakistanu. Bezpośrednią przyczyną było dążenie Pakistanu Wschodniego, tzw. Bengalu Wschodniego, do większej autonomii i ostra, nosząca znamiona pacyfikacyjne, reakcja rządu w Islamabadzie. W wyniku buntu części jednostek wojskowych, wspierających ludność Bengalu, doszło do wybuchu wojny domowej [Dobrzelewski 2016, s. 38]. 17 kwietnia 1971 r. ogłoszono powstanie niepodległego Bangladeszu. Wojska pakistańskie szybko przeszły do ofensywy i pacyfikacji zbuntowanej prowincji. Na masową skalę rozpoczęły się ucieczki mieszkańców Bengalu, którzy szukali schronienia w Indiach. Indie szybko poparły powstanie nowego państwa i udzieliły pomocy uchodźcom, potępiły natomiast Pakistan. Do zaognienia sytuacji doprowadziły naloty pakistańskie na tereny przygraniczne; niektóre z nich wkraczały na terytorium Indii. Indie uznały to za argument do wojny, która rozpoczęła się 3 grudnia. Zawieszenie broni zostało przyjęte 16 grudnia. Działania wojenne miały miejsce również na terenie Kaszmiru, gdzie przewagę osiągnęło wojsko hinduskie. Skutkiem wojny było utworzenie z Pakistanu Wschodniego nowego państwa – Bangladeszu. Rozmowy pokojowe zakończyły się 2 lipca 1972 r. podpisaniem przez premier Indii Indirę Gandhi i prezydenta Pakistanu Zulfikara Ali Bhutto porozumienia w mieście Simla. Porozumienie z Simli przewidywało między innymi rozwiązywanie sporów drogą pokojową, zaniechanie wrogiej propagandy, wznowienie łączności między obydwoma krajami. W rejonie Kaszmiru wyznaczono nową linię demarkacyjną, zwaną „linią kontrolną". W maju 1976 r. Indie i Pakistan ogłosiły przywrócenie stosunków dyplomatycznych i handlowych.

W następnych latach wielokrotnie dochodziło do starć zbrojnych pomiędzy sąsiednimi armiami. W 1997 r. z okazji 50 rocznicy uzyskania niepodległości przez Indie i Pakistan premier rządu pakistańskiego zwrócił się z apelem do władz indyjskich o zorganizowanie w Kaszmirze plebiscytu. Propozycja spotkała się ze zdecydowanym sprzeciwem rządu w Delhi, który wykluczył jakikolwiek porozumienie podważające suwerenne prawa do spornego terytorium. Przełom lat

osiemdziesiątych i dziewięćdziesiątych charakteryzują walki wojsk indyjskich z bojownikami muzułmańskimi nazywającymi siebie „mudżahedinami" (arab. 'święty wojownik'). Odnotowano znaczny wzrost działalności organizacji propakistańskich oraz o charakterze separatystycznym. Wiele dowodów wskazuje, że te pierwsze mają wsparcie rządu w Islamabadzie lub nawet działają z jego inspiracji. Zalicza się do nich między innymi Laskhar-e-Taiba, odpowiedzialna za zamachy w 1993 i 2008 r. oraz Hizb-ul-Mujahideen, uznawana przez GlobalSecurity.org za zbrojne ramię pakistańskiego ISI. Aby się im przeciwstawić, w lipcu 1986 r. Indie rozpoczęły operację Brasstacks – manewry wojskowe, koncentrując do grudnia 1986 r. w przyległym do Pakistanu Radżastanie ponad 150 tysięcy żołnierzy. Pakistan odpowiedział tym samym i sytuacja zaczęła grozić kolejnym konfliktem zbrojnym. W 1999 r. znów doszło do wzrostu napięcia między państwami, które zaniepokoiło opinię międzynarodową, obawiającą się wybuchu czwartej wojny między Indiami a Pakistanem.

W lipcu 1999 r. na skutek zabiegów dyplomatycznych udało się stronom wypracować ugodę i powstrzymać działania kaszmirskich separatystów. Do 2000 r. problem Kaszmiru w stosunkach indyjsko-pakistańskich nie został rozwiązany. Sporne terytorium stanowi punkt zapalny na mapie geopolitycznej świata, wywołujący liczne zamieszki i incydenty zbrojne.

Od momentu zaistnienia konfliktu o Kaszmir obie strony prezentują niezmienne stanowiska polityczne. Pakistan twierdzi, że sporne terytorium stanowi integralną część muzułmańskiego imperium, a w świadomości każdego Pakistańczyka istnieje przekonanie o konieczności podjęcia przez państwo walki o wolność Kaszmiru. Indie podkreślają, że Kaszmir wywodzi się z dawnych księstw hinduskich i stanowi konstytucyjną, niezbywalną część terytorium państwowego. Obie strony prezentują odmienne metody rozstrzygnięcia sporu. Pakistan zdecydowanie opowiada się za przeprowadzeniem plebiscytu na terenie Kaszmiru, w którym ludność zadecydowałaby o przynależności do któregoś z państw (liczy na głosy muzułmanów, stanowiących 80% społeczności). Na krawędzi wojny oba kraje znalazły się ponownie po zamachach na indyjski parlament 13 grudnia 2001 r. Władze w Delhi oskarżyły stronę pakistańską o współudział w zamachach. Przy granicy w Kaszmirze doszło do koncentracji wojsk obu państw, napięcie złagodzono w dużej mierze dzięki mediacjom Stanów Zjednoczonych. Do rozmów pokojowych powrócono na przełomie 2003 i 2004 r. W maju 2003 r. przywrócono stosunki dyplomatyczne, a w listopadzie tego roku weszło w życie zawieszenie broni w Kaszmirze. Kolejne lata przyniosły rozszerzenie współpracy na poziomie gospodarczym i ekonomicznym. Indie i Pakistan współdziałały w niesieniu pomocy ofiarom trzęsienia ziemi

w Kaszmirze w październiku 2005 r. Dzięki temu proces pokojowy był kontynuowany, prowadzono rozmowy na szczeblu ministrów spraw zagranicznych, a z czasem doszło do spotkania prezydenta Asifa Ali Zardariego z premierem Singhiem we wrześniu 2008 r. 21 października b.r. Indie i Pakistan otworzyły nieczynny od pierwszej wojny międzypaństwowej szlak handlowy łączący obie części Kaszmiru.

Problem Kaszmiru był wielokrotnie poruszany na forum Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych (ONZ). Do obu państw wysyłano misje mediacyjne i wydawano rezolucje w celu pokojowego rozwiązania sporu. W 1948 r. Rada powołała komisję mającą za zadanie rozstrzygnięcie sporu między państwami (United Nations Commission for India and Pakistan, tzw. UNCIP) oraz opowiedziała się za przeprowadzeniem referendum na spornym terytorium, pozostawiając decyzję o przynależności do Indii lub Pakistanu ludności kaszmirskiej. Wobec braku zdecydowanej interwencji ONZ w konflikt oba państwa szukały sprzymierzeńców na arenie międzynarodowej. Sojusznikiem Pakistanu zostały Stany Zjednoczone Ameryki Północnej (USA) oraz Chiny, po stronie Indii opowiedział się Związek Socjalistycznych Republik Radzieckich (ZSRR), który stał się rzecznikiem Delhi na arenie międzynarodowej [www.prezi.com/lgmi5rm7igih/konflikt-indyjsko-pakistanski]. Obecnie rząd indyjski dąży do utrzymywania poprawnych stosunków z Rosją. Budując koalicję antyterrorystyczną po zamachach 11 września 2011 r., George W. Bush ocieplił stosunki z Indiami. Tradycyjnie Stany Zjednoczone wspierają Pakistan, który jako państwo islamistyczne prowadzi wobec Zachodu podwójną grę, „po cichu" wspierając terrorystów.

Uregulowanie konfliktu jest w zasadzie pozorne. W 1999 r. doszło do walk w rejonie Kargilu, a w 2016 r. do odwetowych działań wojsk indyjskich za atak terrorystyczny na terytorium przygranicznym w Pakistanie. W czasie pierwszego z wymienionych wydarzeń strony poniosły straty porównywalne do tych z 1971 r. [Dobrzelewski 2016, s. 217; Gorzyński 2016]. Codziennie na linii kontroli indyjsko-pakistańskiej odbywa się ceremonia zamykania granicy. W przeprowadzonych przez autora tekstu wywiadach w czasie badań metodą wywiadu środowisk akademickich i szeroko pojętej inteligencji w 2017 i 2018 r. w Mumbaju i New Dehli, Chandigaru (Czandigaru) i Bangaluru Pakistan wskazywany jest jednoznacznie jako sprawca zamachów terrorystycznych i potencjalne źródło zagrożenia wojennego dla Indii.

Należy tu uwzględnić potencjały militarne obu państw. Amia indyjska to 1,3 mln żołnierzy, 3500 czołgów, 1250 samolotów, 600 śmigłowców i 170 okrętów. Według SIPRI Indie wydają 2,5% PKB na obronność, co daje budżet w wysokości ponad 38 mld USD. Pakistan zaś posiada 650 tys. żołnierzy służby zasadniczej oraz

302 tys. członków organizacji paramilitarnych wyposażonych w ok. 2500 czołgów, 2100 transporterów opancerzonych i ok. 300 śmigłowców oraz blisko 460 samolotów bojowych. Marynarka wojenna jest stosunkowo nieliczna, dysponuje 68 okrętami i 48 samolotami. Kraj wydaje niespełna 5 mld USD na zbrojenia, co stanowi ok. 2,6% PKB. Obie strony dysponują bronią jądrową; Pakistan posiada od 90 do 120 głowic. Pakistan liczy ponad 200 mln mieszkańców, Indie zaś 1,35 mld ludności. Obszar ten znajduje się w polu zainteresowania innego mocarstwa atomowego – Chińskiej Republiki Ludowej, którą zamieszkuje również ponad miliard ludzi. Oznacza to, że potencjalny konflikt w tym regionie objąłby swym zasięgiem 1/3 populacji Ziemi[2].

Indyjskie władze centralne i lokalne wobec wyzwań i zagrożeń bezpieczeństwa wewnętrznego

Złożona sytuacja międzynarodowa i opisywane powyżej zróżnicowanie etniczne wpływają bezpośrednio na bezpieczeństwo wewnętrzne. Kształtowanie bezpieczeństwa wewnętrznego odbywa się zarówno na szczeblu centralnym, jak i rządów stanowych[3].

Rządząca od 2014 r. Bharatiya Janata Party BJP (Indyjska Partia Ludowa) ma charakter narodowy, odwołuje się do tradycji hinduistycznej. Jednak w obszarze gospodarki, nauki i rozwoju społecznego formułuje ambitne cele osiągnięcia poziomu państw wysoko rozwiniętych (UE, USA).

Na szczeblu centralnym identyfikowane są także wyzwania i zagrożenia bezpieczeństwa publicznego i społecznego. Właściwa diagnoza uwzględniać musi takie elementy, jak: populacja – 1 350 000000 (błąd statystyczny 3%), ok. 300 narzeczy, różnorodność religijna, dziedzictwo kolonialne, brak realnych danych dotyczących populacji wielkich miast, w tym skali przestępczości. Badanie dostępnych publikacji, zwłaszcza zaś mediów anglojęzycznych, pozwala stwierdzić, że za najpoważniejsze bolączki uznaje się: rozwarstwienie, pozostałości społeczeństwa kastowego, degradację środowiska naturalnego, brak dostępu znacznej części społeczeństwa do podstawowych zdobyczy cywilizacji, których następstwem są terroryzm, przestępczość zorganizowana i pospolita oraz korupcja.

[2] Szerzej o mocarstwowej pozycji Indii patrz: [Zajączkowski 2008, ss. 104–148].

[3] W przypadku Indii trudno stwierdzić, że jest to bezpieczeństwo lokalne, gdyż poszczególne stany zamieszkiwane są przez populacje porównywalne do państw określanych mianem co najmniej „średnich".

Uporządkowaniu spraw publicznych służy zasada równości wobec prawa, wszystkich obywateli Indii obowiązuje prawo karne. W prawie cywilnym zastosowano zasadę, że jego przepisy wobec obywateli uzależnione są od wyznawanej przez nich religii. Sąd Najwyższy oraz sądy stanowe weryfikują zgodność stanowionego prawa i działań rządu centralnego i rządów stanowych z konstytucją[4].

Na szczeblu centralnym prowadzone są działania mające na celu zwalczanie zarówno przyczyn, jak i skutków negatywnych zjawisk społecznych. Upowszechniana jest akcja „Clean India", którą można tłumaczyć jako *Czyść Indie* lub *Czyste Indie*. Jak podaje portal Cleanindiashow, w 2019 r. odbywa się już 14 edycja działań obejmujących proekologiczne wystawy, promocje i akcje zachęcające zarówno do stosowania „czystych" technologii, jak i najzwyklejszego przestrzegania zasad higieny i sprzątania śmieci. Jednocześnie poruszany jest też wątek dostępu do świeżej wody i toalet. W Indiach, doceniając znaczenie tej sfery bytowej, otwarto pierwsze na świecie muzeum toalet, którego podstawową funkcją jest edukacja. Rząd centralny dąży do upowszechnienia szczepień i edukacji. W 2009 r. przyjęto ustawę, która objęła obowiązkiem szkolnym dzieci w wieku od 6 do 14 lat, a przede wszystkim usprawniła i urealniła system finansowania szkolnictwa (ok. 3% PKB). W ten sposób dąży się do zmniejszenia liczby dzieci nieuczestniczących w zajęciach szkolnych, których liczbę 10 lat temu szacowano na ok. 70 milionów. Inne działania na szczeblu centralnym to upowszechnianie legalnej zabezpieczonej umowami pracy oraz ubezpieczeń społecznych. Na przestrzenie ostatnich lat liczba ubezpieczonych zdrowotnie i emerytalnie wśród osób pracujących wzrosła z ok. 40% do 60%.

Indie są krajem szczególnie zagrożonym przez terrorystów. Wskazują na to zarówno czynniki rządowe, jak i badani metodą ankietową i wywiadu, bez względu na pozycję społeczną i pochodzenie. Terroryzm utożsamiany jest z muzułmanami, a właściwie Pakistańczykami. W praktyce powoduje to napięcia i niechęć do islamskiej mniejszości religijnej, choć nie znajduje to odzwierciedlenia w polityce rządu i rządów stanowych. Zagrożenie terrorystyczne wpływa jednak na wzmożone działania policji, straży granicznej, wojska, ale także bardzo licznych i aktywnych agencji ochrony.

Problemy bezpieczeństwa, w tak rozległym i mającym tak liczną populację kraju, są zróżnicowane terytorialnie. Zjawisko przestępczości pospolitej w badaniach jest powszechnie łączone z dużymi miastami, takimi jak New Delhi i Mumbaj. Jest

[4] Wymiar sprawiedliwości Indii tworzą: Sąd Najwyższy (Supreme Court of India; prezes i 25 sędziów); sądy stanowe (High Courts); stanowe sądy okręgowe; trybunały administracyjne i sądy specjalne [www.msz.gov.pl/pl/p/newdelhi_in_a_pl/wspolpraca_dwustronna/gospodarka_indii/ind_informacje/].

ono trudne do realnego przedstawienia w sposób statystyczny, ponieważ pomimo najlepszych chęci organów ścigania w warunkach megamiast prawdopodobnie większość przestępstw nie jest zgłaszana i opisywana[5]. Rozbieżne są już nawet dane dotyczące liczby mieszkańców (Mumbaj – 18mln–24mln, New Delhi – 22mln–26 mln).

Charakterystyczne zjawiska to: przeludnienie, problemy sanitarne i higieniczne, bezdomność, przestępczość (zwłaszcza seksualna), niekontrolowany napływ imigrantów z terenów wiejskich, bezrobocie, żebractwo itp. Jak podają różne źródła, do wielkich miast codziennie przybywa od 2 do 5 tys. osób z terenów wiejskich, co daje średnio ponad 1 mln przybyszów rocznie. Nie posiadają oni żadnych środków do życia, mieszkają na ulicach, są środowiskiem patologicznym, w którym szerzą się narkomania, prostytucja, przemoc i kradzieże. W celu przeciwdziałania tym zjawiskom podejmowane są takie działania, jak: akcje informacyjne, reklama społeczna, akcje policyjne, karanie przestępców (np. kastracja gwałcicieli), tworzenie stref bezpieczeństwa, akcje społeczne, np. budowa toalet i łaźni.

Istnieją jednak ośrodki miejskie i stany, które zaliczyć można do najbezpieczniejszych na świecie. Przykładem jest Chennai (Madras) zwane „Indyjskim Detroit", z ok. 5 mln mieszkańców. Miasto pod względem wypracowywanego PKB zajmuje 3 miejsce w kraju po Mumabju i New Delhi. Znajduje się tam 1/3 przemysłu Indii. W materiałach promujących miasto można znaleźć informację, że należy ono do 50 najbezpieczniejszych miast świata. W ośrodku tym przyjęto specyficzny model zarządzania przez Chennai Corpration. Zarząd miasta, uwzględniając zarówno tradycje, jak i lewicowe idee ruchu robotniczego, kształtuje życie publiczne poprzez akcje socjalne, finansowanie oświaty i wsparcie działań kulturalnych, prowadzonych zwłaszcza przez fundacje, stowarzyszenia i ośrodki kultury[6].

Innym ciekawym „zjawiskiem" jest społeczność sikhów. Według oficjalnych statystyk sikhowie stanowią 9% 24-milionowej społeczności indyjskiego Pendżabu,

[5] Przykładem może tu być statystyka indyjskiego Narodowego Biura Rejestracji Przestępstw (National Crime Records Bureau, NCRB), które podało, że w 2010 r. popełniono ponad 33 tys. morderstw, a więc o 3% więcej niż w roku poprzednim. Aż o 13,4% wzrosła liczba prób zabójstwa i porwań, wzrosła przestępczość, której ofiarami były kobiety (213 585 zarejestrowanych przypadków w 2010 r.), o ponad 10% wzrosła przestępczość przeciwko dzieciom (26 694). O 5,5% wzrosła liczba ofiar wypadków drogowych. W zeszłym roku życie straciło w ten sposób 133 tys. osób. Odnotowano o 7,7% więcej śmierci w wyniku nieszczęśliwych wypadków i samobójstw. [za: Budyńska 2011]. Z kolei inne źródła wskazują, że ofiarami gwałtów w samych tylko metropoliach pada ponad 700 tys. kobiet.

[6] Na podstawie wywiadu z byłym ministrem stanu Madras ds. oświaty, przeprowadzonego przez autora w kwietniu 2018 r.

jednak w stolicy stanu, mieście Chandigar (Czandigar), są ludnością dominującą, zwłaszcza w sferze kultury i ekonomii[7]. Chandigar to miasto projektu Le Corbusiera, które wybudowano jako stolicę stanu utworzonego po wojnie z Pakistanem w latach siedemdziesiątych. Sikhizm jest eklektyczną religią głoszącą walkę ze złem. Kierująca się przepisami religijnymi społeczność, sama zapobiega większości patologii społecznych, takich jak żebractwo, przestępczość pospolita czy prostytucja, bądź próbuje je zwalczać.

O zróżnicowaniu oceny źródeł zagrożeń świadczy podejście władz poszczególnych stanów do walki z nadużywaniem napojów alkoholowych. Za przykład służyć tu może polityka podatkowa, zróżnicowana lokalnie, która powoduje, że ceny whisky „Signature", będącej jednym z charakterystycznych produktów indyjskich, w 2018 r. kształtowały się, w zależności od regionu, w zakresie od 400 do 2100 rupii indyjskich. Dodać należy, że problem nadmiernego spożywania alkoholu jest jednym z zagrożeń bezpieczeństwa wewnętrznego identyfikowanych na szczeblu centralnym.

Zakończenie

Indie postrzegane są w Europie, a zwłaszcza w Polsce głównie jako cel wypraw turystycznych. Stąd w literaturze, prasie, a nawet w Internecie dominują przekazy skierowane do potencjalnych turystów [Trolese 2018]. Tymczasem jest to kraj ogromnych możliwości, także dla firm z naszej części świata. W rozmowie z autorem w 2017 r. ówczesny konsul generalny Rzeczpospolitej Polskiej w Mumbaju Leszek Brenda prezentował pogląd, że mimo pewnych różnic kulturowych i administracyjnych polskie firmy osiągają sukcesy na rynku indyjskim. Problematyka identyfikowania zagrożeń i wyzwań dla bezpieczeństwa (zewnętrznego i wewnętrznego) Indii oraz sposoby rozwiązywania tych problemów na szczeblu centralnym i lokalnym wymagają dalszych pogłębionych badań.

Autor prezentowanego tekstu zdaje sobie sprawę, że artykuł ma charakter przyczynkarski. Badania na terenie Indii prowadzone w latach 2015–2018 wskazują na bariery, głównie kulturowe i świadomościowe, mieszkańców państwa-subkontynentu. Należy jednak mieć nadzieję, że dalsze prace badawcze przyczynią się do pogłębienia znajomości tematu i upowszechnienia go w materiałach o zasięgu międzynarodowym i krajowym. Wobec dalszego dynamicznego rozwoju Indii celowe jest

[7] Jest to właściwie stolica dwu stanów: Pendżab i Haryna. Miasto liczy ok. 1 mln mieszkańców.

prowadzenie badań dotyczących tego rejonu Azji, także w sferze bezpieczeństwa, gdyż ich wyniki okazać się mogą przydatne dla polskich inwestorów

Bibliografia

Burke J. (2011), *Lepiej nie być kobietą w Delhi*, ,,The Guardian'', 11.03.2011, udostępnione przez Onet.pl.

Budyńska A. (2011), *Wzrost przestępczości w Indiach*, ,,India News'', 28.10.2011 r. [online], www. polska-azja.pl.

Dobrzelewski J. (1971) [2016], *Indie-Pakistan*, Bellona, Warszawa.

Gorzyński O. (2016), *Narastające napięcia między Pakistanem i Indiami. Coraz bliżej wojny* [online], www. wp. Wiadomości, dostęp: 30.09.2016.

Trolese A. (2017), *Podróż do Indii. 30 rzeczy, które warto wiedzieć przed podróżą* [online], https://tasteandtravel.pl/2017/12/05/indie-podroz/, dostęp: 5.12.2017.

Zajączkowski J. (2008), *Indie w stosunkach międzynarodowych*, Wydawnictwo Scholar, Warszawa, ss. 104–148.

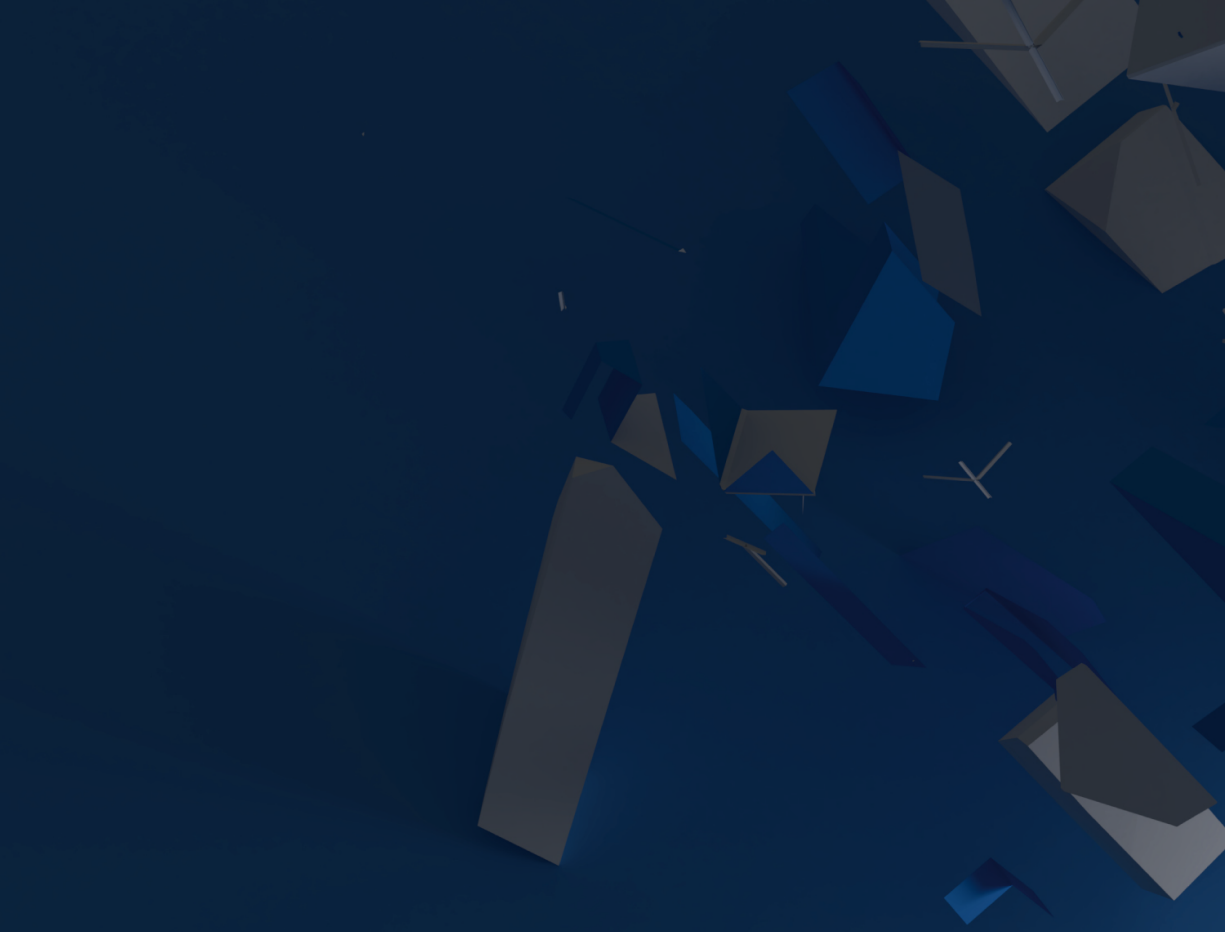
Strony internetowe

www.defence24.pl/

www.msz.gov.pl/pl/p/newdelhi_in_a_pl/wspolpraca_dwustronna/gospodarka_indii/ind_informacje/

www. polska-azja.pl

www.prezi.com/lgmi5rm7igih/konflikt-indyjsko-pakistanski



ISBN **978-83-64971-61-7**

Społeczna Akademia Nauk
Łódź

www.san.edu.pl