Journal of KONBiN 49(2019)
e-ISSN 2083-4608
DOI 10.2478/jok-2019-0014

Sławomir DYGNATOWSKI[1], Paweł DYGNATOWSKI[2],
Łukasz DOMŻAŁ-DRZEWICKI[1]
[1] *Polish Air Force University (Lotnicza Akademia Wojskowa)*
[2] *Air Force Institute of Technology (Instytut Techniczny Wojsk Lotniczych)*

THE ANALYSIS OF USING STRUCTURAL SOLUTIONS IN CYBERSECURITY BASED ON ORCHARD OPERATION

Analiza wykorzystania rozwiązań strukturalnych w obszarze cyberbezpieczeństwa na przykładzie operacji Orchard

Abstract: *The modern battlefield seems to be nothing without the electronic infrastructure. The susceptibility of specific systems to threats from electronic countermeasures or hackers has a substantial influence on the potential conflict. This article describes the measures used by the state of Israel in the field of cybersecurity. Development level of their systems is very high since their relations with neighbours are hostile, constant threat extorted the development of efficient solutions, which were tested on the battlefield. In addition, the article presented the potential course of Orchard operation to demonstrate the correct usage of offensive measures in cyberspace.*
Keywords: cybersecurity, electronic warfare, Orchard operation.

Streszczenie: *Współczesne walki pole nie istnieje bez infrastruktury elektronicznej. Podatność poszczególnych systemów na zagrożenia ze strony środków do prowadzenia wojny elektronicznej lub też włamań dokonywanych przez hakerów ma istotny wpływ na przebieg potencjalnego konfliktu. W poniższym artykule określono środki jakie używa Państwo Izrael w zakresie cyberbezpieczeństwa. Poziom rozwoju ich systemów jest bardzo wysoki, ponieważ ich stosunki dyplomatyczne z sąsiadami są wrogie, stałe zagrożenie wymusiło rozwój skutecznych rozwiązań, które zostały przetestowane na polu walki. Ponadto w artykule zaprezentowano potencjalny przebieg operacji Orchard, aby zademonstrować prawidłowe użycie środków ofensywnych w cybeprzestrzeni.*
Słowa kluczowe: cyberbezpieczeństwo, wojna elektroniczna, operacja Orchard.

1. Introduction

In the era of digitalisation of social life and expansion of the presence of the state in cyberspace, security specialists emphasise the necessity to increase the social awareness and establish the nationwide security strategies.

National strategies on cybersecurity should include well-defined strategical and tactical objectives and accurately designated management should be able to manage the forces and measures to implement tasks given by the political authorities.

Unfortunately, Poland experiences a long-lasting stagnation in this field. Additionally, social awareness in cybersecurity leaves a lot to be desired. According to data from PWC „Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępczością liczą na szczęście" (English: a cyber lottery in Poland. Why the companies rely on luck while combating the cybercrime), in 2017 even 44% of companies made financial losses and 62% of them recorded some disruptions due to the lack of awareness of the necessity of data protection.

Due to the intensity of hazards in cyberspace, recently we witness the attempts to combine the concepts suggested by MSWiA (Ministry of Internal Affairs and Administration), MON (Ministry of Defence), Ministerstwo Cyfryzacji (Ministry of Digitalisation) as well as the cyber security specialists, whose aim is to consolidate the authority over the sector in one place. The concept also includes the statement of the government plenipotentiary for cybersecurity holding the rank of the undersecretary or the secretary of state in the Ministry of National Defence. The tasks of the plenipotentiary include:

- Analysis and assessment of cybersecurity based on the accumulated data and indicators developed with the participation of government bodies and reaction teams responding to incidents of computer security, operating at the Ministry of National Defence, Agency of Internal Security as well as Scientific and Student Computer Network – National Research Institute;
- Reaching new solutions and initiating actions in the area of ensuring cybersecurity at the national level;
- Submitting opinions of legal acts and other government documents affecting the implementation of tasks in the area of cybersecurity;
- Running and coordinating actions conducted by government administration bodies aimed at raising social awareness on threats of cybersecurity and safe usage of the Internet;
- Collaborating in the field of cybersecurity with other countries, organisations and international institutions;

- Taking actions aimed at supporting research and development of technology in the field of cybersecurity.

Due to the broad range of the issues, a question arises whether directing the central decision core to the resort structure of national defence is the appropriate step, considering the extensive civilian usage of the cyberspace. In some countries, e.g. in Latvia, such a model does not exist.

Another organisational model of structures associated with cybersecurity is observed, e.g. in Great Britain or Israel. The high priority of this sector in structures of state security emphasises the fact of the subordination to their Prime Minister. In Isreal, the NCD (National Cyber Directorate) is subordinated in this way. In Great Britain, GCHQ (Government Communications Headquarters) and NCSC (National Cyber Security Centre) has been added to the structure related with security in cyberspace.

Worldwide there are different organisation models of cybersecurity sector in state structures. This organisation depends on the rank of objectives associated with security in cyberspace in the state's structures.

The investment in secure cyberspace sector provides specific benefits. It enables the development of one's own economy, not only related to IT segment. It has to be stressed that substantial amounts were spent on this sector by Estonia during a dispute from 2007 between Russia and Estonia. Protection costs against low and medium-level attacks of the Russian empire (or elements originating from this country), e.g. DDoS (distributed denial of service) attacks reached the amount of 424 USD for every dollar spent by the attacking party.

The aim of the analysis is to demonstrate the possibility of using the structural solutions and cyber attacks based on the experience of Isreal and the response to question whether the application of electronic (ECM) and cybercrime countermeasures has an impact on reducing the reliability of the country's air defence, which may result in a failure to run strategic projects of the country under attack.

2. The activity of Israel in the field of cybersecurity

The state of Isreal is distinguished by highly developed cyber systems. The reason for this is a permanent risk of potential attacks of their neighbours, with whom the diplomatic relations are hostile or at least unfriendly. The aim of this article is not to analyse the appropriateness of this or that posture of Israel, but to accentuate how civilian and military structures are capable of meeting air targets by the state's management in cyberspace sector.

The foundations of the protection system of critically important infrastructure facilities were laid at the turn of the XX and XXI century. It was then decided to create a security system in this field.

The most essential feature of this system is its flexibility – no rigid operational windows are established. The changing work environment initiates the adaptation of the structure. Israel led to the creation of the so-called ecosystem, which includes human capital, science and industry. Besides, there is a division into sector activities, i.e. civilian sector in charge of the protection of the critically important infrastructure facilities and military sector: for the protection of one's own systems, as well as offensive actions. The priority of these solutions is strengthened not only by developing competencies of state's structures dealing with security in cyberspace but also by annual meetings of this sector with the inaugural speech of the Prime Minister as well as offensive actions conducted by Israel. The result of these actions is to maintain a close correlation and flexibility between specific elements of the ecosystem. It provides with the possibility to efficiently react to various events.

It is worth elucidating that the actions of Israel in cyberspace are specific in the light of the global activity of the countries. It is involved not only in the activity targeted at protecting its own systems or typical intelligence activity - gathering information, but also an offensive activity with its preemptive actions. This action can be defined as a sum of intelligence activities with the potential offensive response. Due to the broad spectrum of behaviours of Israel, it comes top of the countries with offensive and defensive capabilities in cyberspace, just like Russian Federation, United States or the People's Republic of China.

The functioning of Israel in cyberspace can be well exemplified based on the analysis of Orchard operation from 2007.

3. Orchard operation

The intervention of Israel in 2007 on the territory of the Syrian Arab Republic was caused by a plethora of factors. We will focus in particular on political and economic events, that were an attempt to isolate Syria from up to seven years back from the intervention in question.

The isolation process should be associated with a wide range of actions undertaken by Israel and the increasing role of the United States at that time, the closest ally of Israel, on the territory of the Middle East. It was the time of the enhanced control by the USA and its allies in the territory of Iran as well as isolating an important ally of Syria – Iran. For Syria, a country ruled by family clans and with

a high level of pride as well as grand plans for the expansion of their influences, were sufficient to take more and more bold steps. Unfortunately, they were not supported by one's own position in the region. A substantial element was the attempt to strengthen one's position by maintaining the resources of chemical warfare and the effort to gain access to nuclear power. The plan was preserved in strict secrecy because every event of information disclosure could result in serious consequences for Syria, the least severe option would be grave economic repercussions from Israel and the USA.

Already in the 80s of the XX century, the Syrian Arab Republic tried to obtain the technology enabling the production of nuclear power, but the XXI century and establishing contacts with the Democratic People's Republic of Korea does brought about a change in this field. Among others, the attempt to build in Syria a reactor enabling the production of plutonium, in the long run, was aimed at establishing cooperation. This reactor was placed on a desert area in the vicinity of Dajr az-Zaur. Another significant event, which allowed to speed up works on a nuclear weapon by Damascus was the American intervention in 2003. According to a variety of reports, it resulted in the escape of a portion of scientists dealing with nuclear technology on Syrian territory. According to the reports of the US Intelligence Agency, the authorities in Damascus managed to contact with Abdul Qadeer Khan (the founder of the Pakistani atomic programme). In terms of the security of Israel, the wide range of the aforementioned activities of Syria could be indicative of the expected future threat to the interests and security of Israel. Besides, the increased cooperation of Damascus authorities with Hezbollah's structures and the ongoing consolidation of the relationship with Iran leads to the cultivation of a permanent hostile posture in mutual relations.

Currently, there is no information available on how the operation was conducted, nor which measures were used for its implementation, but it is possible to outline future scenarios with a certain degree of probability. Previously the software has to be presented, which is capable of generating interferences of the correct radar operation. As mentioned above, the collaboration of Isreal and National Security Agency (NSA) could result in the application of SUTER programme, of which up to the attack three generations were made. SUTER I enabled to monitor what enemy radars see. The second generation allowed to take control over the enemy network and its sensors. The third generation enabled to seize the full control of network systems, including rocket launchers and radars, reinforcing in consequence operator's false convictions about correct operation of the system. The Syrian anti-aircraft defence at the time possessed mostly Russian equipment of Buk-M1 SAM missile system, introduced into service in 1979. Usually, the equipment of this class, despite its age, is suitable for use, but the topic of our deliberations is the

attack on electronic equipment utilising the software. The age of machines used by Syria facilitated the penetration of their securities because it is not possible to write a perfect code resilient to any kind of attacks and modifications. If we add to it above 25 years for tests and code acquisition, we come to the conclusion that it is a system, the security breach of which has already occurred. The question arises whether forces and measures needed to neutralise such object with the means of such attack are adequate. Not to mention the fact that security programmers also strive to detect all software gaps; thus the constant use of the measures such as SUTER would end in intercepting the transmission and counteracting its effects. Therefore, it is recommended to treat the measures of this kind as an ace up one's sleeve.

The operation takes place in London and begins with the interception of information from the laptop in 2006. According to the sources, the information was captured in England, where a highly qualified scientist, Ibrahim Othman, was located by agents from the Mossad. He concealed his identity under a fake name, but a hotel reservation system, which was monitored by intelligence services, detected his name as potentially interesting. It indicates that the agents from Mossad presumably keep the guest list on the UK territory constantly under surveillance. When the true identity of the suspect was confirmed, the group of agents was sent to kill the scientist and intercept all the information that he possessed. The group was divided into three groups. The task of the first group was to locate and identify the target as soon as he lands at the London-Heathrow airport. The second group was aimed at keeping a hotel room and all its belongings under surveillance. The last group was intended to follow the target and track its location. The group of agents consisted of qualified killers, burglars, technicians and computer programmers. On the first day, when the scientist was attending a meeting at the Syrian embassy, some agents broke into his hotel room and found an unattended laptop. All data from hard discs were extracted and copied. After that, the computer was provided with special tracking software. When the content was deciphered and the materials were analysed, the officials found building plans and images of Kibar installation at different stages of construction. The amount of the obtained data and its significance resulted in the change of mission objective. The information revealed the level of Syrian atomic programme, and it was decided, so as not to arouse any suspicion, to resign from killing the scientist and let him leave the UK territory with the infected computer. Besides, the Mossad informed CIA of the acquired materials and thanks to the cooperation of both agencies it was found out that Syria and North Korea plan to build a nuclear reactor site. Iran transferred to the project above billion of dollars and intended to use the nuclear rector Kibar to replace one's own installations incapable of enriching uranium.

As can be seen from the above actions, in the modern world it is very challenging to stay anonymous, even for the countries which take pride in the efficient intelligence service and generous operational budget. It cannot be said that Syrian neglected security issues regarding the departure of VIP. Unfortunately, even the best defences are as strong as its weakest link, which is, in this case, a human. The situation could have been prevented if the material were copied on the small encrypted disc and carried it along with oneself. Presumably, a laptop has weak security defences, because it served as a working tool for a person, who used it every day. The daily necessity to connect to an encrypted disc was a real nuisance, to the same extent as using a password containing a lot of signs. A significant amount of materials on the laptop's disc was also an oversight. The person like this, expecting an interference of the third persons, shall be equipped with the minimum materials indispensable for work. It is a negligence of the services, which should investigate the laptop prior to his departure in view of potentially hazardous materials.

Possessing data from laptop and site location, Israelis and Americans began large-scale actions aimed at obtaining further information on the current state of works on the nuclear programme and the confirmation of the acquired data. A spy was successfully hired to the Syrian programme and the employees already working there were also recruited. The scope of the enterprise can be confirmed by the fact that Israel launched a Ofek-7 satellite only to trace the activity over the Syrian nuclear reactor. To make sure that the appropriate installation is being under surveillance, a commando unit disguised as Syrians was sent in the neighbourhood of the facility to take samples of the soil located in the vicinity of the reactor to check whether they are not of the increased radiation level. With the undisputable evidence originating from different sources at their disposal, it was decided to preventively destruct the nuclear reactor to prevent from the advancement of works on his technology. It should be emphasised that all actions undertaken by Israel were in effect to devastate the nuclear reactor.

The operation was conducted at night of 5 to 6 November 2007, but assuming from the precision of the execution and a total neutralisation of the anti-aircraft defence forces, its planning should have dated a lot of months back. The amount of information collected previously and the scrupulousness with which they are accumulated enabled to outline the scenario of attack. Thanks to the satellite reconnaissance, Israeli forces were fully aware of the location of the anti-aircraft defence system of Syria. The enemy's territory had to be monitored by the spies, which infiltrated the defence structures in this area. Thanks to the fact that the system was distinguished by a centralised command station, a person with physical access to the terminal with the use of malware, could infect the connected stations without

any difficulties and efficiently paralyse the possibility to detect the enemy's air vehicles. To make sure the mission will work, Israel reportedly provided all air vehicles with WRE gun pods with SUTER software of the third generation, applied by Americans, which, in case of a failure of detection of software by Syrians would enable to finish a raid. The action was preceded by sending a commando unit, which was instructed to irradiate a laser beam of the nuclear reactor to ensure a target hit with high precision. At night, unit of F-15 and F-16 fighters encroached the Syrian airspace while flying at the low altitude, approximately 100m above the level of the sea. It didn't encounter any difficulties and 45 minutes after midnight it reported the destruction of a nuclear reactor.

4. Summary

The above operation shows the high importance of the battle in cyberspace. Using force in the form of armed air vehicles is the last stage of the battle and constitutes a crowning achievement and outstanding performance of intelligence service as well as programmers/hackers. The whole operation started upon detection of a fake name by a hotel reservation system. Then, the negligence in the area of cybersecurity, lack of training courses for the personnel abandoning the country and consent that personnel would not adhere to guidelines, enabled the foreign intelligence service to come into the possession of information of strategic importance. Besides, it has to be stated that leaving a laptop containing classified information without any supervision, appears to be downright reckless and irresponsible, since even high-standard hotel rooms does not guarantee adequate protection, the same applies to all safes located in the hotels. Unfortunately, they only give us the illusory feeling of safety because most of them can be accessed with an administration code enabling the hotel staff to enter its interior without the guest's consent and awareness. Referring to the disruption operation of anti-aircraft defence system itself, it shall be noted that currently to conduct an effective attack it is no longer necessary to know any of the programming languages and the attack can be executed by a person without any educational background, ranging from a private to a cleaning lady working at the installation. The only thing that is needed is the physical access to the machine and placing the carrier infected with a malware software embedded in an unsecured computer port. In this case, the only way of protecting oneself from the above acts is to have a good, trusted administrator, who will be able to continuously monitor the network traffic and have appropriate tools for system diagnosis and anomaly detection. Furthermore, a crucial factor is to establish adequate procedures aimed at testing the system and its readability, thanks to which

it will be more probable to detect a malicious software or the attack and be diligent in following these procedures, because an everyday routine, haste, and neglecting various scans is an ally of the hacker. It is indispensable to create a special unit, which, in case of hazard detection by local administrators or system operators, will develop methods of counteracting and initiate measures to combat an enemy.

5. References

1. Lakomy M., Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw. Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
2. Medvedev S.A.: Offense-defense theory analysis of Russian cyber capability. Monterey, California: Naval Postgraduate School.
3. Rozporządzenie Rady Ministrów z dnia 16 marca 2018 r. w sprawie ustanowienia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa.
4. http://www.cyberdefence24.pl/cyberbezpieczenstwo-cywilne-czy-wojskowe-analiza, dostęp 24.03.2018.
5. http://www.cyberdefence24.pl/polityka-i-prawo/pulkownik-malecki-system-cyberbezpieczenstwa-izraela-to-dobry-wzor-do-nasladowania, dostęp 24.03.2018.
6. http://www.cyberdefence24.pl/premier-ustanowil-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-, dostęp 24.03.2018.
7. http://www.defence24.pl/odtajnienie-izraelskiego-ataku-na-syryjski-reaktor-nieprzypadkowy-moment, dostęp 25.03.2018.
8. http://www.defence24.pl/sowiecka-rakieta-zestrzelila-izraelski-f-16, dostęp 25.03.2018.
9. https://businessinsider.com.pl/firmy/zarzadzanie/pwc-raport-o-cyberbezpieczenstwie-w-firmach/hrsevwb, dostęp 24.03.2018.
10. https://niebezpiecznik.pl/post/bad-rabbit-czyli-atak-ulepszona-notpetya-ktory-zaszyfrowal-dane-na-ukrainie-w-rosji-oraz-w-polsce/, dostęp 25.03.2018.

ANALIZA WYKORZYSTANIA ROZWIĄZAŃ STRUKTURALNYCH W OBSZARZE CYBERBEZPIECZEŃSTWA NA PRZYKŁADZIE OPERACJI ORCHARD

1. Wprowadzenie

W dobie cyfryzacji życia społecznego, jak i przede wszystkim poszerzania obecności państwa w cyberprzestrzeni, specjaliści od bezpieczeństwa alarmują o konieczności zwiększania świadomości społecznej oraz tworzenia ogólnonarodowych strategii bezpieczeństwa.

Narodowe strategie cyberbezpieczeństwa powinny mieć jasno sprecyzowane cele strategiczne, taktyczne oraz precyzyjnie wyznaczone kierownictwo, umożliwiające gospodarowanie siłami i środkami w celu realizowania wyznaczonych przez władzę zwierzchnią (polityczną) zadań.

W Polsce widoczna jest długoletnia stagnacja w tym obszarze. Dodatkowo świadomość społeczeństwa w kwestii ochrony cybernetycznej nie jest wysoka. Według danych PwC „Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępczością liczą na szczęście", w 2017 r. aż 44% firm poniosło straty finansowe, a 62% odnotowało zakłócenia z powodu braku świadomości o konieczności ochrony danych.

W związku z nasileniem zagrożeń w cyberprzestrzeni, w ostatnim czasie jesteśmy świadkami próby połączenia koncepcji wysuwanych przez MSWiA, MON, Ministerstwo Cyfryzacji, a z drugiej strony specjalistów od bezpieczeństwa w cyberprzestrzeni, której celem ma być konsolidacja władzy nad tym sektorem w jednym miejscu. W koncepcji pojawia się stanowisko Pełnomocnika Rządu ds. Cyberbezpieczeństwa w randze podsekretarza lub sekretarza stanu w Ministerstwie Obrony Narodowej. Do zadań pełnomocnika należeć ma:

- analiza i ocena stanu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji rządowej oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego działających w Ministerstwie Obrony Narodowej, Agencji Bezpie-

czeństwa Wewnętrznego oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym;
- opracowywanie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym;
- opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa;
- prowadzenie i koordynowanie działań prowadzonych przez organy administracji rządowej mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu;
- współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi;
- podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa.

Ze względu na obszerność problematyki rodzi się pytanie: na ile skierowanie głównego trzonu decyzyjnego do struktury resortu obrony narodowej jest posunięciem prawidłowym, mając na uwadze szerokie cywilne wykorzystanie cyberprzestrzeni? W niektórych państwach, np. na Łotwie, taki model funkcjonuje.

Inny model organizacji struktur związanych z cyberbezpieczeństwem obserwujemy np. w Wielkiej Brytanii czy Izraelu. Priorytetowość tego sektora w strukturach bezpieczeństwa państwa podkreśla fakt podległości ich premierowi rządu. W Izraelu w ten sposób podporządkowany jest NCD (National Cyber Directoriate). W Wielkiej Brytanii zaś do struktury związanych z bezpieczeństwem w cyberprzestrzeni zostały dodane, GCHQ (Government Communications Headquarters) i NCSC (National Cyber Security Centre).

Na świecie obserwujemy różne modele organizacji sektora cyberbezpieczeństwa w strukturach państwa. Organizacja ta zależy od rangi celów związanych z bezpieczeństwem w cyberprzestrzeni w określonym państwie.

Inwestycja w sektor bezpieczeństwa w cyberprzestrzeni daje określone korzyści. Umożliwia rozwój własnej gospodarki, nie tylko związanej z segmentem IT. Na uwagę zasługuje fakt wydatkowania na ten sektor znacznych kwot przez Estonię w czasie sporu Estonia–Rosja z 2007 r. Koszt ochrony przed słabo i średniozaawansowanymi atakami strony rosyjskiej (lub elementów pochodzących z tego kraju), m.in. atakami DDoS sięgał rzędu 424 USD na każdy dolar wydany przez stronę atakującą.

Celem analizy jest przedstawienie możliwości wykorzystania rozwiązań strukturalnych oraz ataków cybernetycznych na przykładzie doświadczeń Izraela oraz odpowiedź na pytanie:

Czy zastosowanie środków do walki elektronicznej i cybernetycznej ma wpływ na osłabienie niezawodności funkcjonowania obrony powietrznej kraju, co może skutkować niezrealizowaniem strategicznych projektów atakowanego państwa?

2. Działalność Izraela w zakresie cyberbezpieczeństwa

Państwo Izrael charakteryzuje się wysokim poziomem rozwoju własnych systemów cybernetycznych. Jest to podyktowane permanentnym zagrożeniem potencjalnymi atakami ze strony sąsiadów, z którymi stosunki dyplomatyczne układają się wrogo bądź co najmniej nieprzyjaźnie. Celem tego artykułu nie jest poddanie analizie celowości takiej czy innej postawy Izraela, lecz zobrazowanie, w jaki sposób struktury cywilne i wojskowe są w stanie realizować cele powierzone przez kierownictwo państwa w sektorze cyberprzestrzeni.

Podwaliny pod system ochrony infrastruktury krytycznej i działań ofensywnych w cyberprzestrzeni zostały położone na przełomie XX i XXI wieku. Postanowiono wtedy stworzyć system bezpieczeństwa w tym obszarze.

Najistotniejszą cechą, jaką ów system się charakteryzuje, jest jego elastyczność – nie są tworzone sztywne ramy działań. Zmieniające się środowisko pracy inicjuje dostosowywanie się struktury. Izrael w swych założeniach doprowadził do stworzenia tzw. ekosystemu, w skład którego wchodzi kapitał ludzki, nauka oraz przemysł. Dodatkowo występuje podział na działania sektorowe, tzn. sektor cywilny odpowiedzialny jest za zabezpieczenie infrastruktury krytycznej, zaś wojskowy za ochronę własnych systemów, jak i działania ofensywne. Priorytetowość tych rozwiązań jest wzmacniana nie tylko przez poszerzanie kompetencji struktur państwowych zajmujących się bezpieczeństwem w cyberprzestrzeni, ale również przez coroczne spotkania tego sektora z inaugurującym wystąpieniem premiera, a także działania ofensywne prowadzone przez Izrael. Rezultatem tych działań jest utrzymanie ścisłego powiązania oraz zachowania płynności między poszczególnymi elementami ekosystemu. Daje to możliwość efektywnego reagowania na zdarzenia.

Oczywiście czynności realizowane przez Izrael w cyberprzestrzeni są specyficzne z punktu widzenia globalnej aktywność państw. Wykazuje on nie tylko działalność zabezpieczającą własne systemy czy też działalność typowo wywiadowczą – pozyskiwanie informacji, ale również ofensywą z charaktery-stycznymi dla siebie działaniami wyprzedzającymi. Działanie te możemy zdefiniować jako sumę czynności wywiadowczych z ewentualną ofensywną odpowiedzią. Ze względu właśnie na szerokie spectrum zachowań Izraela, kraj ten plasowany jest w czołówce

państw wykazujących zdolności ofensywne i defensywne w zakresie cyberprzestrzeni, obok Federacji Rosyjskiej, Stanów Zjednoczonych, czy Chińskiej Republiki Ludowej.

Dobrym przykładem do pokazania funkcjonowania Izraela w cyberprzestrzeni jest analiza operacji Orchard z 2007 r.

3. Operacja Orchard

Interwencja Izraela w roku 2007 na terenie Syryjskiej Republiki Arabskiej spowodowana była szeregiem czynników. Skupimy się przede wszystkim na wydarzeniach politycznych i gospodarczych będących próbą izolacji Syrii, z okresu do 7 lat wstecz względem omawianej interwencji.

Proces izolacji należy wiązać z szeregiem działań podejmowanych przez Izrael oraz z rosnącą w ówczesnym okresie rolą Stanów Zjednoczonych – najbliższego sojusznika Izraela, na obszarze Bliskiego Wschodu. Był to czas wzmożonej kontroli przez USA i jego sojuszników terenu Iraku oraz izolowania istotnego sojusznika Syrii – Iranu. Dla Syrii, kraju rządzonego przez klany rodzinne, o wysokim poziomie własnej dumy, jak i szerokich planach rozwoju swoich wpływów, były to wystarczające czynniki do wykonywania coraz to śmielszych kroków. Niestety niepopartych własną pozycją w regionie. Istotnym elementem była próba ugruntowania swojej pozycji poprzez utrzymywanie zasobów broni chemicznej oraz próba uzyskania dostępu do broni jądrowej. Plan był utrzymywany w ścisłej tajemnicy, ponieważ każde ujawnienie informacji mogłoby przysporzyć Syrii – w opcji najmniej dotkliwej – ostrych reperkusji gospodarczych ze strony Izraela oraz USA.

Syryjska Republika Arabska już w latach 80. XX wieku usiłowała pozyskać technologię umożliwiającą produkcję broni jądrowej, jednak to okres XXI wieku i nawiązanie kontaktów z Koreańską Republiką Ludowo-Demokratyczną spowodowało drgnięcie w tej sferze. Między innymi celem nawiązanej współpracy była próba budowy na terenie Syrii reaktora umożliwiającego produkcję w dalszej perspektywie plutonu. Reaktor ten został zlokalizowany na terenie pustynnym w okolicach Dajr az-Zaur. Kolejnym istotnym wydarzeniem umożliwiającym przyspieszenie prac nad bronią jądrową przez Damaszek była amerykańska interwencja w Iraku w 2003 r. Według różnych doniesień spowodowała ona ucieczkę części naukowców zajmujących się technologią nuklearną właśnie na teren Syrii. Władzom w Damaszku, wg doniesień agencji wywiadowczej USA, udało się również nawiązać kontakt z Abdulem Qadeerem Khanem (twórcą pakistańskiego programu atomowego). Z punktu widzenia bezpieczeństwa Izraela szereg wymienionych powyżej działań Syrii świadczyć mógł o spodziewanym przyszłym zagrożeniu dla

interesów, jak i bezpieczeństwa państwa Izrael. Dodatkowo nasilona współpraca władz Damaszku ze strukturami m.in. Hezbollahu oraz nieustanne pogłębianie relacji z Iranem powoduje utrzymanie permanentnego wrogiego stosunku w obustronnych relacjach.

Obecnie nie ma informacji o dokładnym sposobie przeprowadzenia operacji ani o środkach zastosowanych do jej realizacji, jednak można z pewnym prawdopodobieństwem nakreślić scenariusze. Wcześniej należy przedstawić oprogramowanie zdolne generować zakłócenia prawidłowego funkcjonowania radarów. Jak wspomniano wyżej, współpraca Izraela i Agencji NSA mogła zaowocować wykorzystaniem programu SUTER, którego do chwili ataku powstały trzy generacje. SUTER I pozwalał na monitorowanie, co wrogi operator widzi na radarze. Druga generacja pozwalała na przejęcie kontroli nad wrogą siecią oraz jej sensorami. Trzecia generacja pozwalała przejąć pełną kontrolę nad systemami znajdującymi się w sieci, w tym wyrzutniami rakiet oraz radarami, budując w konsekwencji u operatora złudne przeświadczenie, że system działa prawidłowo. Syryjskie siły opl w tym czasie dysponowały w większości rosyjskim sprzętem typu Buk-M1 SAM, wprowadzanym do użytku od roku 1979. Normalnie sprzęt tej klasy pomimo upływu lat nadaje się do wykorzystywania, jednak tematem naszych rozważań jest atak na urządzenia elektroniczne za pomocą oprogramowania. Wiek maszyn używanych przez Syrię ułatwił penetrację ich zabezpieczeń, gdyż nie da się napisać kodu doskonałego odpornego na wszelkiego typu ataki i modyfikacje. Gdy dołożymy do tego ponad 25 lat na testy i pozyskanie kodu, zdamy sobie sprawę, że jest to system, którego zabezpieczenia zostały już złamane. Nasuwa się pytanie, czy siły i środki potrzebne do neutralizacji takiego obiektu za pomocą takiego ataku są adekwatne. Należy pamiętać, że programiści odpowiadający za bezpieczeństwo też starają się wykryć wszystkie luki w oprogramowaniu, dlatego nagminne stosowanie środków typu SUTER zaowocowałoby przechwyceniem transmisji i przeciwdziałaniem jej skutkom. Należy więc traktować środki tego typu jako as z rękawa.

Geneza operacji ma miejsce w Londynie i zaczyna się od przechwycenia informacji z laptopa w 2006 r. Zgodnie ze źródłami, do przechwycenia informacji doszło w Anglii, gdzie wysokiej rangi naukowiec Ibrahim Othman został namierzony przez agentów Mossadu. Ukrywał się on pod fałszywym nazwiskiem, jednak z systemu rezerwacji hotelowych, który był monitorowany przez służby wywiadowcze, jego nazwisko zostało wychwycone jako potencjalnie interesujące. Świadczy to o tym, że najprawdopodobniej agenci Mossadu stale inwigilują listę gości na terytorium UK. Po potwierdzeniu prawdziwej tożsamości podejrzanego została wysłana grupa agentów, której celem było zlikwidowanie naukowca oraz przechwycenie wszelkich informacji będących w jego posiadaniu. Grupa została podzielona na trzy części. Pierwsza miała za zadanie namierzyć i zidentyfikować cel

zaraz po tym, jak wyląduje na lotnisku Heathrow. Zadaniem drugiej była inwigilacja pokoju hotelowego i wszystkich rzeczy znajdujących się w nim. Ostatnia miała za zadanie podążać za celem i monitorować jego położenie. Grupa agentów składała się z wyspecjalizowanych zabójców, włamywaczy oraz techników i informatyków. Pierwszego dnia, podczas gdy naukowiec odwiedzał syryjską ambasadę, część agentów włamała się do jego pokoju hotelowego i znalazła laptopa. Wszystkie dane z dysków twardych zostały zgrane, a na komputerze zainstalowano specjalne oprogramowanie służące do monitorowania dalszej aktywności. Po rozszyfrowaniu zwartości dysków i przeanalizowaniu materiałów, urzędnicy znaleźli plany budynków oraz zdjęcia placówki Kibar w różnych fazach budowy. Ilość zdobytych danych oraz ich znaczenie spowodowały zmianę celów misji. Informacje pokazywały poziom syryjskiego programu atomowego, zdecydowano więc, żeby nie wzbudzać podejrzeń, zrezygnować z zabójstwa naukowca i pozwolono mu wraz z zainfekowanym laptopem na opuszczenie UK. Co więcej, Mossad poinformował CIA o zdobytych materiałach i dzięki współpracy obu agencji wywiadowczych odkryto, że Syria wraz z Północną Koreą oraz Iranem budują placówkę reaktora jądrowego. Iran przekazał na projekt ponad bilion dolarów oraz planował użycie reaktora jądrowego Kibar do zastąpienia własnych placówek niezdolnych do wzbogacenia uranu.

Z zarysu powyższych działań widać, że we współczesnym świecie bardzo trudno utrzymać anonimowość nawet państwom dysponującym sprawnym kontrwywiadem oraz dużym budżetem operacyjnym. Nie można powiedzieć, że Syryjczycy zaniedbali kwestie bezpieczeństwa związanego z samym wyjazdem VIP-a. Niestety nawet najlepsze zabezpieczenia są tak silne, jak najsłabsze ich ogniwo, a w tym przypadku człowiek. Sytuacji można by uniknąć poprzez przeniesienie materiału na mały zaszyfrowany dysk i noszenie go ze sobą. Prawdopodobnie laptop był słabo zabezpieczony, ponieważ służył jako narzędzie pracy człowiekowi, który używał go codziennie. Potrzeba codziennego podłączenia zaszyfrowanego dysku zewnętrznego była zwykłą uciążliwością, tak samo jak stosowanie hasła złożonego z dużej liczby znaków. Duża ilość materiałów na dysku laptopa też była niedopatrzeniem. Osoba tego pokroju, spodziewająca się ingerencji osób trzecich, powinna mieć minimum materiałów niezbędnych do pracy. Jest to zaniedbanie służb, które przed wyjazdem powinny zbadać laptopa pod kątem materiałów potencjalnie niebezpiecznych.

Dysponując danymi z laptopa oraz położeniem placówki, Izraelczycy oraz Amerykanie rozpoczęli szeroko zakrojone akcje mające na celu pozyskanie dalszych informacji o aktualnym stanie prac nad programem atomowym oraz potwierdzenie zdobytych danych. Do syryjskiego programu udało się zatrudnić szpiega

oraz zwerbować już pracujących tam pracowników. O skali przedsięwzięcia powinien świadczyć fakt, że Izrael wystrzelił satelitę Ofek-7 tylko i wyłącznie po to, by śledził aktywność nad syryjskim reaktorem jądrowym. Aby zyskać pewność, że obserwowany jest właściwy kompleks, w pobliże został wysłany odział komandosów przebranych za Syryjczyków, którego celem było pobranie próbek gleby z okolic kompleksu do sprawdzenia, czy nie mają podniesionego poziomu promieniowania. Dysponując niepodważalnymi dowodami pochodzącymi z różnych źródeł, podjęto decyzję o prewencyjnym zniszczeniu reaktora, aby zapobiec postępowi prac na technologią. Należy podkreślić, że prawdopodobnie wszystkie działania podjęte przez Izrael miały w konsekwencji doprowadzić do zniszczenia reaktora.

Sama operacja została przeprowadzona w nocy z 5 na 6 listopada 2007 r., jednak wnioskując z precyzji wykonania oraz całkowitej neutralizacji sił opl, jej planowanie musiało sięgać wielu miesięcy wstecz. Ilość informacji zdobytych wcześniej i skrupulatność, z jaką zostały pozyskane, pozwalają z dużą dozą nakreślić scenariusz samego starcia. Dzięki zwiadowi satelitarnemu siły Izraela doskonale znały rozmieszczenie systemu opl Syrii. Na terenie przeciwnika na pewno działali szpiedzy, którzy przeniknęli do struktur obrony na tym obszarze. Dzięki temu, że system charakteryzował się scentralizowanym stanowiskiem dowodzenia, osoba z fizycznym dostępem do terminala za pomocą złośliwego oprogramowania bez większych problemów mogła z jednego punktu zainfekować wszystkie przyłączone do niego stanowiska, skutecznie paraliżując możliwość wykrycia wrogich statków powietrznych. Aby mieć pewność powodzenia misji, Izrael prawdopodobnie wyposażył dodatkowo wszystkie samoloty w zasobniki WRE z oprogramowaniem SUTER wersji trzeciej, stosowane przez Amerykanów, co w przypadku porażki lub wykrycia oprogramowania przez Syryjczyków pozwoliłoby na dokończenie rajdu. Akcja została poprzedzona wysłaniem oddziału komandosów, których zadaniem było opromieniowanie wiązką lasera reaktora jądrowego, aby umożliwić precyzyjne trafienie bombami. Nocą przestrzeń syryjską naruszył zespół myśliwców F-15 oraz F-16, lecących na niskim pułapie, w granicach 100 m nad poziomem morza. Nie spotkał on żadnych problemów i 45 minut po północy zameldował zniszczenie reaktora jądrowego.

4. Podsumowanie

Powyższa operacja pokazuje, jak duże znaczenie ma walka w cyberprzestrzeni. Użycie siły w postaci uzbrojonych statków powietrznych pojawia się na samym końcu i stanowi ukoronowanie działania wywiadu oraz programistów/hakerów. Cała operacja zaczęła się od namierzenia fałszywego nazwiska poprzez system

ewidencji gości hotelowych. Następnie zaniedbania w zakresie cyberbezpie-czeństwa, brak szkoleń dla personelu opuszczającego kraj lub przyzwolenie, aby personel nie zastosował się do zaleceń, umożliwiły obcemu wywiadowi wejście w posiadanie informacji o znaczeniu strategicznym. Należy w tym wypadku stwierdzić, że pozostawienie laptopa z tajnymi informacjami bez nadzoru jest skrajnie nieodpowiedzialne, gdyż hotelowe pokoje nawet o wysokim standardzie nie zapewniają dostatecznego zabezpieczenia, to samo tyczy się wszystkich sejfów znajdujących się w hotelach. Dają one iluzoryczne poczucie bezpieczeństwa, gdyż większość z nich ma kod administracyjny umożlwiający personelowi otwarcie go bez zgody i wiedzy gościa. Przechodząc do samej operacji zakłócenia działania systemu opl, należy podkreślić, że w obecnych czasach do przeprowadzenia skutecznego ataku nie jest wymagana znajomość jakichkolwiek języków programowania, a ataku może dokonać osoba bez żadnego wykształcenia, zaczynając od szeregowca po sprzątaczkę pracującą w kompleksie. Wystarczy fizyczny dostęp do sprzętu oraz umieszczenie nośnika ze złośliwym oprogramowaniem w niezabezpieczonym porcie komputera. W tym wypadku jedynym sposobem na obronę jest posiadanie dobrego administratora, zdolnego do ciągłego monitorowania ruchu sieciowego, wyposażonego w odpowiednie narzędzia do diagnozowania systemu i wykrywania anomalii. Ponadto istotnym czynnikiem jest wypracowanie odpowiednich procedur mających na celu testowanie systemu oraz jego gotowości, dzięki czemu bardziej prawdopodobne będzie wykrycie złośliwego oprogramowania lub ataku, oraz sumienne ich przestrzeganie, ponieważ codzienna rutyna, pośpiech, bagatelizowanie męczących skanów systemu jest sprzymierzeńcem hakera. Nieodzowne jest stworzenie specjalnej jednostki, która w przypadku wykrycia zagrożenia przez lokalnych administratorów bądź operatorów systemów, opracuje szybko metody przeciwdziałania, oraz sama rozpocznie działania wymierzone w przeciwnika.

5. Literatura

1. Lakomy M., Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw. Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
2. Medvedev S.A.: Offense-defense theory analysis of Russian cyber capability. Monterey, California: Naval Postgraduate School.
3. Rozporządzenie Rady Ministrów z dnia 16 marca 2018 r. w sprawie ustanowienia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa.
4. http://www.cyberdefence24.pl/cyberbezpieczenstwo-cywilne-czy-wojskowe-analiza, dostęp 24.03.2018.
5. http://www.cyberdefence24.pl/polityka-i-prawo/pulkownik-malecki-system-cyber-bezpieczenstwa-izraela-to-dobry-wzor-do-nasladowania, dostęp 24.03.2018.

6. http://www.cyberdefence24.pl/premier-ustanowil-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-, dostęp 24.03.2018.
7. http://www.defence24.pl/odtajnienie-izraelskiego-ataku-na-syryjski-reaktor-nieprzypadkowy-moment, dostęp 25.03.2018.
8. http://www.defence24.pl/sowiecka-rakieta-zestrzelila-izraelski-f-16, dostęp 25.03.2018.
9. https://businessinsider.com.pl/firmy/zarzadzanie/pwc-raport-o-cyberbezpieczenstwie-w-firmach/hrsevwb dostęp 24.03.2018.
10. https://niebezpiecznik.pl/post/bad-rabbit-czyli-atak-ulepszona-notpetya-ktory-zaszyfrowal-dane-na-ukrainie-w-rosji-oraz-w-polsce/, dostęp 25.03.2018.