Tomasz Mielko*

Could Pegasus Gate have been prevented? The evolution of the export control regime for cyber-surveillance tools in Israel

Abstract

The subject of this article is a discussion of the legal provisions governing the Israeli and international legal systems governing the control of trade in cyber-surveillance tools. A detailed analysis of the current regulations is carried out with a view to classification and pointing out imperfections in the content of the current regulations. The author identifies the transformations in the content of the Wassenaar Arrangement, which resulted in an attempt to regulate this matter more comprehensively in Israeli law in 2016. Using the impact of the international NSO software scandal as an example, the role that an effective export control regime, including international regulation, plays in preventing cyber-surveillance tools from being used in ways that are dangerous to internationally recognized values is demonstrated.

Key words: cyber-surveillance, export control, Wassenaar Arrangement, cyber defence

* Tomasz Mielko is a lawyer in Miller Canfield global law firm. He specializes in defense and security matters, export controls, and public procurement law, e-mail: t.mielko@wp.pl, ORCID: 0000-0002-4863-6230.

For many years, with successive discoveries and technological advances, questions have been raised about the need to restrict access to effective and dangerous cyber tools against certain states as well as private actors who may use such tools to disrupt international peace and security, violate human rights or achieve goals politically and militarily contrary to the interests of the producer country. The problem is multidimensional, as the recent global espionage scandal involving the flagship software of the Israeli manufacturer NSO Group, the Pegasus system, vividly demonstrates. The scale of the excitement generated by the 2021 revelations of attacks using this system on journalists, opposition figures, lawyers, human rights activists, and the wider political opposition in many countries around the world, has completely obscured the important issue of controlling the proliferation of cyber surveillance systems and has not sufficiently prompted a discussion of the political and legal measures that should be implemented in the future to ensure that offensive cyber tools are used as a last resort, in a manner that is appropriate and fit for purpose.

This paper will discuss the internal and international legal regime under which the export of Israeli-made offensive cyber-surveillance tools, including the software known as the Pegasus system, takes place, taking into account developments in legislation covering Israeli export controls. This text will also focus on demonstrating the role that an effective export control system, including international regulations, plays in preventing the use of cyber surveillance tools in ways that are dangerous to internationally recognized values.

The current growing rivalry between major powers and the changes in the world order resulting from the transition to a multilateral order are resulting in an exponential demand by states for effective means of conducting offensive as well as defensive operations in a new war space – the cyber domain. This sphere, as was the case at the beginning of the 20th century with the advent of military aviation, is not yet fully regulated in international law, although noteworthy efforts are being made to produce universally applicable rules for the use of cyber weapons, or to interpret the law already in force in this area[1]. For the time being, the boundary between a state of war and peace in

1 Noteworthy documents include: M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2017; *The future of discussions on ICTs and cyberspace at the UN*, 10.08.2020, https://tiny.pl/95bk8 [access: 20.09.2022]. It should be noted that the UN Group of Governmental Experts on the Development of Responsible State Behaviour in Cyberspace in the Context of International Security was established, https://tiny.pl/95b29 [access: 20.09.2022].

the cyber domain is not yet clear, nor is it fostered by the attitude of many actors in the international arena, who are not interested in drawing a thin red line that would unambiguously allow these states to be separated from each other. Such trends are undoubtedly influencing the development of a huge cyber defense market in Israel[2].

A number of regional factors are also noteworthy, such as the continuing sense of insecurity for the state of Israel, the strong emphasis on private sector-state cooperation, the opening of offices of multinational corporations such as Oracle, Dell, IBM and Deutsche Telekom within the Advanced Technology Park, along with research and development centers. Israel also attaches great importance to the study of cyber-security, classes in this subject are taught in schools, and universities and the state also offers the possibility of obtaining a PhD in this field. Extremely interestingly, it is one of the few countries that uses its own armed forces as an incubator for the development of start-ups. High-quality professionals trained in military centers go into business after completing their service, combining business with the benefit of state security. Given the factors presented, enabling Israel to be counted as a powerhouse in terms of capabilities in the cyber domain, it is clear that the country is making an effort to support its own entrepreneurs in the ever-growing global cyber defence market[3]. The implications of the close link between this highly sensitive industry and the institutions and key interests of the state are extremely momentous[4].

Controlling the export of cyber surveillance products in Israel encounters severe restrictions, which are to some extent market-driven – cyber defence entrepreneurs are not interested in imposing additional restrictions and obligations on them, having the effect of limiting potential markets only to countries that guarantee an adequate level of respect for civil rights and freedoms. Another issue remains the political decisions of the Israeli government in this highly sensitive area, as selling, or refusing to sell, or even withholding access to software at the time of special operations can be part

2 S. Shulman, *As cyber wars escalates Israeli tech gains an edge*', CTech, 2.04.2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3902572,00.html [access: 21.09.2022].

3 J. Vadakkanmarveettil, *Why the Israelis lead the world in cyber security expertise*, Jigsawacademy, 27.01.2020, https://www.jigsawacademy.com/why-the-israelis-lead-the-world-in-cyber-security-expertise/ [access: 21.09.2022].

4 L. Tabansky, I. Ben Israel, *Cybersecurity in Israel*, New York 2015.

of the shaping of international relations, including political pressure on the entities to which such software has been offered.

In approaching the international legal regulations relating to export controls in Israel, it is important to point to binding international treaties relating to arms trade controls, among them: The Nuclear Non-Proliferation Treaty (NPT), the Biological Weapons Convention (BWC), the Chemical Weapons Convention (CWC), the Arms Trade Treaty (ATT), or the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW), and non-binding multilateral export control agreements such as the Australia Group (AG), the Nuclear Suppliers Group (NSG), the Missile Technology Control Regime (MTCR), and the Wassenaar Arrangement.

It is important to point out that only the Wassenaar Arrangement[5] refers to export control mechanisms for cyber-surveillance technologies, and that control regulations for such technologies were introduced in December 2013[6]. This amendment, by adding two categories to the control list, now includes „intrusion software" and certain „IP network communications surveillance systems or equipment", these categories having been introduced in sections 4.A.5 and 5.A.1.j) respectively.

By definition „intrusion software" is software specifically designed or modified to evade detection by monitoring tools or to defeat the protective countermeasures of a network-capable computer or device, and meeting any of the following criteria: a. extracting data or information from, or modifying system or user data in, a network-capable computer or device; or b. modifying a standard execution path of a program or process to enable the execution of externally supplied instructions. In contrast, „IP network communications surveillance systems or equipment, and specially designed components therefor", having all of the following: 1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone): a. Analysis at the application layer [e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1)]; b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and c. Indexing of extracted data; and 2. Being specially designed to carry out all of the following:

5 Full text in English is available at https://www.wassenaar.org/control-lists/ [access: 21.09.2021].

6 I. Pyetranker, *An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement*, „Northwestern Journal of Technology and Intellectual Property" 2015, vol. 13/2, no. 3, p. 152–180.

a. Execution of searches on the basis of „hard selectors"; and b. Mapping of the relational network of an individual or of a group of people. 5.A.1.j. does not apply to systems or equipment, specially designed for any of the following: a. Marketing purpose; b. Network Quality of Service (QoS); or c. Quality of Experience (QoE).

Separately, the Wassenaar Arrangement also refers to cyber systems with strictly military applications, which are defined in the Munitions List under category ML.21.b.5. As proposed in the text of the Agreement, the definition of the indicated category is software specifically designed or modified for military offensive cyber operations. In addition, it is indicated that ML21.b.5. includes software designed to destroy, damage, degrade or disrupt systems, equipment or software as defined in the Munitions List, Cyber Reconnaissance and Cyber Command and Control. ML21.b.5. does not apply to vulnerability disclosure or cyber incident response limited to non-military defence preparedness or cyber security response. Given the nature of the software as defined in ML21.b.5 of the Wassenaar Arrangement Weapons List, it should be considered that the NSO Group's product does not fall within this type of software, as it is, according to the available information, designed to covertly infect the recipient's device, mainly a phone, and the software does not have the kinetic effects characteristic of the products defined in provision ML21.b.5 of the Weapons List. In classifying the Pegasus software produced by the NSO Group, it should be pointed out that, in light of the Wassenaar Arrangement, only software specifically designed, or modified, to generate, command and control or deliver „intrusion software" is on the Dual-Use List, as indicated in para. 4.D.4. Thus, Pegasus software, in the light of the Wassenaar Arrangement, does not fall into the category of armaments, nor does it fall into any category of dual-use items. Nevertheless, from a technical point of view, it is undisputed that the Pegasus software itself also requires equipment and technology to retrieve data from infected devices, possibly also to process the retrieved data and technical support equipment. Given the wording of the Wassenaar Arrangement regulations, the Pegasus system may require authorization as a dual-use product to the extent that Category 4.D.4. specifies that software and devices that are complementary within the Pegasus system infrastructure require authorization.

In view of the findings already made, it should be pointed out that the lists contained in the Wassenaar Arrangement, being non-binding, require implementation into the national legal order of the signatory states. This is most often done by extending the lists of dual-use items or weapon lists

in the legislation of the country concerned with the new categories adopted under the Arrangement. The specific legal language of the Arrangement has resulted in official guides being published in many countries around the world to enable exporters to verify whether their product falls under the export control regulations[7].

The legal regime adopted in Israel in this regard is unique. Although the country is not formally a member of the Wassenaar Arrangement, domestic legislation, the Defence Export Control Law (DECL)[8], directly references the Wassenaar Arrangement's list of arms and dual-use goods and technologies, with the exception of information security technologies (encryption devices). Israel is therefore treated as a compliant state, which is significant given that arms sales from Israel place the country among the top ten global exporters of such products. In addition to this, the DECL law authorised the Knesset to enact a national systematic list of arms and dual-use items, in accordance with the Annex to the Defence Export Control Regulation[9]. The body responsible for issuing export licences is the Defence Export Control Agency (DECA) within the Israeli Ministry of Defence, which issues licences for various defence-related goods and technologies, as well as dual-use items for national security purposes. Controlling the export of dual-use items for civilian end-users is the responsibility of the Israeli Ministry of Economy, which additionally also issues licences for the export of items related to sensitive goods and technologies: chemical, biological and nuclear, in addition, this body controls the export of Unmanned Aerial Vehicles and many other listed items. The export of cryptographic equipment is the responsibility of an autonomous unit of the Encryption Control Department at DECA[10]. Cryptographic assets are subject to a different legal regime, and the export control unit has overall oversight of cryptography issues, including responsibility for research and development of encryption techniques and devices. Israel applies a relatively simplified

7 An example is the guidance issued by the US Bureau of Industry and Security – https://www.bis.doc.gov/index.php/guidance [access: 21.09.2022].

8 Defense Export Control Law (Journal of Laws 2007, 5777 no. 274, p. 186) as amended, https://www.nevo.co.il/law_html/law01/999_796.htm [access: 21.09.2022].

9 Annex to the Defense Export Control Order, Combat Equipment & Controlled Dual-Use Equipment. KT 5640 no. 6640 of 1/13/2008, p. 348, https://www.nevo.co.il/law_html/law01/999_890.htm [access: 21.09.2022].

10 For more information on the jurisdiction of export control authorities in Israel: N. Margolis, *Work in progress? Israeli export control regulators face up to new challenges*, „WorldECR" 2021, issue 102, p. 28–30.

system of sanctions and embargoes, which is overseen by the Israeli Ministry of Finance.

The amendment of the Wassenaar Arrangement at the end of 2013 took the cyber market in Israel by surprise because, unlike in most countries, the Arrangement is directly binding in Israel and triggered by law the effect of having to place cyber-surveillance tools under export controls. At the same time, work was underway in the Israeli Ministry of Defence to comprehensively regulate the export control of products falling into the categories of „intrusion software" and „IP network communications surveillance systems or device", as part of internal regulations implementing and detailing the content of the provisions of the Wassenaar Arrangement in question.

In early 2016, a draft act emerged that established a broad regulatory framework for the export of cyber products[11]. This draft law included much broader export controls than is the case under the Wassenaar Arrangement standards, including to the extent that the Arrangement (section 4.D.4) does not include controls on products or devices on which software is run or stored[12]. The Israeli Defence Ministry also proposed to extend the definition of „intrusion software" to include certain products that can cause disruption to systems or any physical damage to a system. The draft regulation also included controls on the export (transmission) of exploits, cyber tools related to the military sphere and espionage and digital forensics devices. However, the important and, in retrospect, expedient draft was rejected, due to the highly critical stance taken by representatives of the Israeli cyber-military-industrial complex. Noteworthy for the arguments raised, industry representatives feared that the proposed regulation would restrict market access, lead to an exodus of talented professionals, reduce the competitiveness of Israeli companies in the industry, and consequently stagnate the dynamics of the rapidly growing cyber defence market, in which Israel is a global powerhouse. In the end, in the face of unified opposition from the industry, the draft regulation was rejected, leaving cyber surveillance software exporters with the possibility

11 D. Hindin, *Can Export Controls Tame Cyber Technology?: An Israeli Approach*, Lawfare, 12.02.2016, https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach [access: 21.09.2022].

12 A. Iliescu, *Israeli import, export, cyber regulation & enforcement*, Shibolet law, 19.05.2020, https://www.shibolet.com/en/israeli-import-export-and-cyber-regulation-and-enforcement/ [access: 21.09.2022].

of obtaining exemptions from the need to obtain export licences[13]. Given the extreme importance of the cyber industry and its close connection to state security interests, there was a tendency in Israel to deregulate and streamline as much as possible the export licensing process for cyber surveillance and cyber security tools.

Consequently, given that Israeli export control regulations do not restrict the export of cyber-surveillance tools due to the requirement to respect human rights in a particular country – offensive cyber surveillance tools have been sold to many countries around the world where standards of protection of human rights and fundamental freedoms are not guaranteed at a sufficiently high level. Although the activities of the NSO Group described above have been widely criticised, it must be recognised that the export of cyber surveillance tools by Israeli companies has complied with both national law and the Waasenaar Agreement, and therefore arguments sometimes made about the sale of cyberweapons to non-democratic countries should be regarded as unjustified under current law. Nevertheless, the DECL regulations, which do not in any way refer to the condition of respecting human rights in the country to which the export is made, should be regarded as a sham because, as a consequence, the adopted model, although formally allowing exporters to act within the limits of national and international law – violated the non formally binding standards of the international community.

In 2019 NSO Group reported that it has implemented an extensive compliance program internally to implement the principles of the UN Guiding Principles on Business and Human Rights. The company also has policies in place to protect human rights. The purpose of the 2019 – originated program is to address human rights violations within the business, and the controls used to achieve this are multi-stage. The primary tools used for compliance screening are due diligence and risk analysis, both in terms of customers and the category of product sold. The decision to sell a product is taken by a special committee chaired by the NSO President, the company's board of directors has the right to object in this respect. If the manufacturer receives information about an incident of infringement, the manufacturer proceeds to investigate the incident. If the information about the use of the software contrary to the contract or local law is confirmed – the manufacturer may terminate the

13 Y. Azulai, *Natanjahu scraps plans to regulate cybersecurity*, Globes, 19.04.2016, https://en.globes.co.il/en/article-netanyahu-scraps-plans-to-regulate-cyber-security-cos-1001118937 [access: 21.09.2022].

user's access to the software. In January 2021 NSO published its first ever „Transparency and Accountability Report", in which it reported extensively on the measures taken to protect human rights[14].

In November 2021, in response to incoming reports of NSO software being used against US security interests – the US Department of Commerce blacklisted the manufacturer of Pegasus, resulting in a ban on any US companies selling technology to NSO Group and its subsidiaries, at the same time Shalev Hulio, founder and CEO of NSO Group resigned to continue in office[15]. On 6 December 2021 DECA issued a statement announcing that the number of countries to which cyberweapons can be exported has been reduced from 102 to 37[16], in addition, the content of the end-user declaration has changed. Now, any contractor of Israeli companies exporting cyber-surveillance tools commits to using offensive cyber surveillance software only for counter-terrorism and combating serious crimes. Breach of the commitment results in the loss of the licence, including the exclusion of the software in the course of the mission, which undoubtedly constitutes a severe sanction for the purchaser's beneficial secret services.

The past year has been an exceptionally eventful and dynamic one for the cyber defence industry, and it seems that the series of major international scandals caused by NSO Group and its flagship software will serve as a warning to other cyber-surveillance tool makers. Not so long ago, NSO was at the center of French investor interest, only to find itself in dire financial straits a year later, lose its founder and be placed on the US Department of Commerce's sanctions list. Given the dynamic and continuous growth of the market for cyber-surveillance tools, as well as the fusion of cyber interests with the existential interests of rival states, as highlighted here on several occasions, there is no need to be optimistic about a moratorium on cyber weapons, or even more control over their proliferation. Export control regulations on their own may prove to be an insufficient measure to prevent advanced cyber-surveillance tools from being misused for their official purpose, but

14 *Transparency and Accountability Report 2021*, https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [access: 22.09.2022].

15 K. Huang, *Chief of Israeli Spyware Firm NSO to Step Down as It Revamps*, New York Times, 21.08.2021, https://www.nytimes.com/2022/08/21/business/nso-chief-executive-spyware.html [access: 22.09.2022].

16 Ch. Forrester, *Israel tightens regulations around cyber exports*, Janes.com, 7.12.2021, https://www.janes.com/defence-news/news-detail/israel-tightens-regulations-around-cyber-exports [access: 22.09.2022].

it is no less important to recognise that a milestone in this regard is the introduction of the new Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. New export control regulations for cyber-surveillance tools have also come into force in the United States, with new items added to the CCL list as of 19 January 2022 and additional definitions added to The Export Administration Regulations (EAR)[17]. The proposed changes aim to prohibit the sale of offensive cyber surveillance tools to authoritarian countries, including Russia and China.

The extremely interesting yet controversial example of the indirect influence of the interests of NSOs and similar companies on the content of export control regulation in Israel shows that leaving cyber-surveillance tools essentially out of effective control within the controlled trade is a profitable solution only in the very short term. There are many indications that the Israelis, who have so far led the way in developing cyber-surveillance tools, will be forced to give way to competitors who are far better able to exercise discretion around their activities without leading to their systems being used in a way that is widely objectionable. The political background to the decision to restrict the limit of countries to which exports of cyber surveillance tools from Israeli manufacturers are possible is also indicated by media reports of a significant reduction in the issuing of export licences and thus „starving the industry"[18]. It remains to be believed that Pegasus Gate will have a strong impact on the manufacturers of offensive cyber surveillance tools and that it will bring about the implementation of corporate mechanisms that will prevent scandals and thus the use of such tools will only be allowed as a last resort and against real threats to the functioning of democratic states.

17 Read more about the NSO acquisition plans *France and Israel hold 'secret' talks to defuse phone spyware row*, The Guardian, 22.10.2021, https://www.theguardian.com/world/2021/oct/22/france-and-israel-hold-secret-talks-to-defuse-phone-spyware-row [access: 23.09.2022].

18 The current state of the industry for cyber surveillance is described in an article A. Gilead, *Export controls strangling Israel's cyberattack industry*, Globes, 25.04.2022, https://en.globes.co.il/en/article-tighter-export-controls-strangling-israels-cyberattack-sector-1001410066 [access: 23.09.2022].

Bibliography

Azulai Y., *Natanjahu scraps plans to regulate cybersecurity*, Globes, 19.04.2016, https://en.globes.co.il/en/article-netanyahu-scraps-plans-to-regulate-cyber-security-cos-1001118937 [access: 21.09.2022].

Cornish P., *The Oxford Handbook of Cyber Security*, Oxford 2021.

Eichensehr K.E., *Public-private cybersecurity*, „Texas Law Review" 2017, vol. 95.

Forrester Ch., *Israel tightens regulations around cyber exports*, Janes.com, 7.12.2021, https://www.janes.com/defence-news/news-detail/israel-tightens-regulations-around-cyber-exports [access: 22.09.2022].

France and Israel hold 'secret' talks to defuse phone spyware row, The Guardian, 22.10.2021, https://www.theguardian.com/world/2021/oct/22/france-and-israel-hold-secret-talks-to-defuse-phone-spyware-row [access: 23.09.2022].

Gilead A., *Export controls strangling Israel's cyberattack industry*, Globes, 25.04.2022, https://en.globes.co.il/en/article-tighter-export-controls-strangling-israels-cyberattack-sector-1001410066 [access: 23.09.2022].

Hindin D., *Can Export Controls Tame Cyber Technology?: An Israeli Approach*, Lawfare, 12.02.2016, https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach [access: 21.09.2022].

Huang K., *Chief of Israeli Spyware Firm NSO to Step Down as It Revamps*, New York Times, 21.08.2021, https://www.nytimes.com/2022/08/21/business/nso-chief-executive-spyware.html [access: 22.09.2022].

Iliescu A., *Israeli import, export, cyber regulation & enforcement*, Shibolet law, 19.05.2020, https://www.shibolet.com/en/israeli-import-export-and-cyber-regulation-and-enforcement/ [access: 21.09.2022].

Margolis N., *Work in progress? Israeli export control regulators face up to new challenges*, „WorldECR" 2021, issue 102.

Pyetranker I., An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement, „Northwestern Journal of Technology and Intellectual Property" 2015, vol. 13/2, no. 3.

Schmitt M., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2017.

Shulman S., *As cyber wars escalates Israeli tech gains an edge'*, CTech, 2.04.2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3902572,00.html [access: 21.09.2022].

Tabansky L., Ben Israel I., *Cybersecurity in Israel*, New York 2015.

The future of discussions on ICTs and cyberspace at the UN, 10.08.2020, https://tiny.pl/95bk8 [access: 20.09.2022].

Transparency and Accountability Report 2021, https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [access: 22.09.2022].

Vadakkanmarveettil J., *Why the Israelis lead the world in cyber security expertise*, Jigsawacademy, 27.01.2020, https://www.jigsawacademy.com/why-the-israelis-lead-the-world-in-cyber-security-expertise/ [access: 21.09.2022].

Czy można było zapobiec Pegasus Gate? Ewolucja systemu kontroli eksportu narzędzi do cyberinwigilacji w Izraelu

Streszczenie

Przedmiotem niniejszego artykułu jest omówienie przepisów prawnych regulujących w izraelskim i międzynarodowym systemie prawnym kontrolę obrotu narzędziami służącymi do cyberinwigilacji. Przeprowadzona została szczegółowa analiza obowiązujących regulacji, której celem jest klasyfikacja i wskazanie niedoskonałości w treści obowiązujących przepisów. Autor identyfikuje zmiany w treści porozumienia z Wassenaar, które spowodowały, że w 2016 roku podjęto próbę bardziej kompleksowego uregulowania kontroli obrotu narzędziami do cyberinwigilacji w prawie izraelskim. Na przykładzie skutków międzynarodowej afery z oprogramowaniem NSO autor pokazuje rolę skutecznego reżimu kontroli eksportu, w tym regulacji międzynarodowych, w zapobieganiu wykorzystywania narzędzi służących do cyberinwigilacji w sposób niebezpieczny dla wartości uznawanych na arenie międzynarodowej.

Słowa kluczowe: cybernadzór, kontrola eksportu, porozumienie z Wassenaar, cyberobrona