Article

Trimming Pegasus' Wings

International Export Control Law and 'Cyberweapons'

27.10.2021

For centuries, export control regulations have accompanied the development of new weapon technologies. The revelations of the 'Pegasus Project' have put the question of whether and how to regulate the export of the new technology 'cyberweapons' in the limelight: Is the current international export control law up to the challenge of sufficiently regulating the proliferation of 'cyberweapons' or does it need an update? To answer this question, the blog post will, first, turn to the definition and relevance of 'cyberweapons'. Secondly, international export control law is introduced as a possible measure to mitigate the risks posed by 'cyberweapons' against the backdrop of regulating the use of 'cyberweapons' or establishing a moratorium on its trade. Third, the blog post will assess the export of 'cyberweapons' in general and the export of Pegasus in particular within the current international export control framework. The current framework seems to touch upon partial aspects of the trade with 'cyberweapons'. However, it stands to fear that it is not up to the task of sufficiently curtailing the proliferation of 'cyberweapons' and the associated risks, as it especially leaves the underlying problem of the trade with zero-day vulnerabilities untouched.

The 'Pegasus Project'

The 'Pegasus Project' is an investigative research project into the dealings of the Israeli company NSO Group Technologies (NSO). NSO is a technology firm that sells a smartphone surveillance tool called 'Pegasus' to States. The States can then silently – thus without user interaction of the target like 'clicking' on a link (so-called zero-touch) – install 'Pegasus' on smartphones, taking advantage of unknown software vulnerabilities (so-called zero-day vulnerabilities). The combination of zero-day and zero-touch can be referenced as zero-day zero-touch vulnerabilities, which are particularly rare and valuable. After successful intrusion, the intruder can access the smartphone's data, communications, and turn on the microphone, the camera, and GPS tracking. The project revealed that many States used the tool not only to legitimately fight crime and terrorism but also to spy on human rights attorneys, journalists, activists, opposition politicians, dissidents, and other State's officials. While such *use* by the recipient state raises *inter alia* the issue of the legality of international espionage, the following sections will address whether the *transfer* of 'Pegasus' has violated international export control law.

Defining 'Cyberweapons'

Amid the revelations, 'Pegasus' has often been referred to as a 'cyberweapon' (see, i.e., here, here and here). However, it is unclear what the term 'cyberweapon' precisely conveys. So far, a clear-cut (legal) definition has not emerged. Instead, 'cyberweapons' are primarily described in varying functional or technical terms. One point of divergence is the distinction between *offensive* and *defensive* cyber tools and whether they both fall within the category of 'cyberweapons'. Moreover, it is unsettled whether surveillance tools like 'Pegasus' should be classified as 'cyberweapons'. However, for this blog post, a precise delimitation is unwarranted as this classification does not affect the assessment of surveillance tools under international export control law.

The interconnected world is undoubtedly vulnerable to attacks by 'cyberweapons'. They pose significant risks to critical infrastructure, the functioning of the State, international peace and security, and — like 'Pegasus' — to individuals' human rights. Despite these risks, the trade of 'cyberweapons' flourishes due to high demand by States and other actors. The copying and electronic transfer of 'cyberweapons' further

accelerate their proliferation compared to traditional arms. One way to cope with these risks is to regulate the *use* of 'cyberweapons' and promote responsible state behavior in cyberspace.

Regulating the Use of 'Cyberweapons'?

In the last years, several state and non-state initiatives have started addressing the problem in different fora and with different focuses. These include the 'UN Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security' (OEWG), the 'UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security' (GGE), the 'Programme of Action for Advancing Responsible State Behaviour in Cyberspace', the Tallinn Manual Processes (with 3.0. just being initiated) and state practice (i.e. Germany).

State practice, thereby, concentrates mostly on applying current international law to cyberspace, including issues surrounding 'cyberattacks'. Germany, for example, is of the position that cyber operations by a state may infringe upon another state's rights and may likewise be responded to by cyber means, i.e., to counter an armed (cyber-)attack. Moreover, Germany puts forward that cyber operations need to and are able to follow IHL when employed. Similarly, the Tallinn Manual focuses on applying the international law of war to cyberspace, including the application to cyberattacks perpetrated with 'cyberweapons'. In contrast, the GGE and the OEWG not only deal with the application of international law to cyberspace but also established detailed, non-binding norms to advance 'Responsible State Behaviour in Cyberspace in the Context of International Security'. History, however, has shown that mere regulation on the use of certain technologies and weapons does not suffice to prevent actors from 'irresponsibly' utilizing the technology to the detriment of international peace and security. Therefore, these actors need to be barred from acquiring 'cyberweapons' in the first place.

An International Moratorium on the Trade with 'Cyberweapons'?

Prominently, Edward Snowden called for an international export ban on 'cyberweapons' amid the 'Pegasus' revelations (see similarly here, here, here, here and here). Such a ban seems like an apparent solution to the proliferation risks associated with 'cyberweapons'. However, such a 'cyberweapons' moratorium is unlikely to emerge in the near-term future for several reasons.

Recent examples show that an international treaty on the issue would most probably require years of lengthy negotiations. For example, the discussions on the regulation on lethal autonomous weapon systems (LAWS) within the United Nations Convention of Certain Conventional Weapons framework have been going on for several years, without significant progress. States' positions regarding this matter range — comparable to the discussion about 'cyberweapons' — from an outright ban of LAWS to 'merely' regulating the trade of LAWS or its components and to not regulating LAWS at all. Moreover, attempts to negotiate a 'Cybersecurity'-Treaty, which would also take on the trade with 'cyberweapons', has so far fallen on deaf ears within the international community.

Nevertheless, the GGE and OEWG took a small step towards a proliferation halt. Their final reports both called for the prevention of 'the proliferation of malicious [information and communications technology] tools and techniques and the use of harmful hidden functions' (see here and here). The GGE thereby restated its principle 13 i), which it had established in its 2015 report, and which has been reiterated by the UN General Assembly (UNGA) on several occasions. These non-binding norms may have an impact towards the creation of formal international law in the future, if they are referenced and reiterated by States and international organs like the UNGA. The Tallinn Manual, for instance, may not be explicitly endorsed by States but is still used as a reference, as exemplified by Germany's report on the application of international law in cyberspace. Despite this, the calls by the OEWG and GGE are merely non-binding recommendations that have not manifested to international law or developed into a comprehensive framework for cyber non-proliferation efforts. For the moment, principle 13 i) reflects the international communities' general understanding that 'cyberweapons' may pose risks to international security and stresses the preference of States for non-binding instruments in this area. This way, they retain enough leeway to foster their strategic goals by exporting 'cyberweapons'. The export of 'Pegasus', for instance, was part of Israeli foreign policy, especially in the warming relations to its Arabic neighbors (see here).

For the same strategic reasons, unilateral declarations by States to impose a moratorium on 'cyberweapons' exports within their jurisdiction are highly unlikely.

While 'new' international law is not on the horizon, the question arises: What does existing international export control law have to say about 'cyberweapons'?

Existing International Export Control Law and 'Cyberweapons'

There are two main pillars in international export control law: binding international arms treaties (i.e., NPT, BTWC, CWC, ATT, CCW) and non-binding multilateral export control regimes (i.e., NSG, Australia Group, MTCR and the Wassenaar Arrangement). These frameworks cover a wide range of weapons, namely nuclear, biological, chemical, and conventional weapons, as well as dual-use items. However, among them, only the Wassenaar Arrangement deals — at least partially — with 'cyberweapons', although without expressly mentioning the term.

The Wassenaar Arrangement is a voluntary export control regime established in 1996, with currently 42 participating States. Its primary purpose is 'to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations.' To this end, the participating States should apply export controls to all items either on the Dual-Use List or the Munitions List, meaning they have to license the export of listed items.

In the case of the Wassenaar Agreement's applicability, States agreed to follow multiple best practices, such as to control the transfer of 'software' irrespective of its means of transfer, thus, including intangible transfers. Moreover, according to the Arrangement, States should report on their export decisions of listed items. If one State denies the export of a listed item, another participating State can still approve the export. The exporting State should then merely notify all other States of the approval. The final export decision always remains the sole responsibility of each participating State.

The Case of 'Pegasus'

In the case of 'Pegasus', Israel claims to have acted 'in accordance with its defense export control law, complying with international export control regimes'. The claim is intriguing as Israel is not a participating State of the Wassenaar Arrangement. However, Israel has committed to following the Arrangement unilaterally. The commitment indicates the authority and impact of the non-binding Wassenaar Arrangement, but only if Israel indeed *acts* within the Arrangement's constraints. Otherwise, Israel's commitment would not be more than mere lip service. Therefore, the question remains whether Israel acted within the bounds of the Wassenaar Arrangement concerning the export of 'Pegasus'.

The Wassenaar Agreement's Munitions List names '"Software" specially designed or modified for the conduct of military offensive cyber operations' as a controlled item (Item 21.b.5. Munitions List). This 'includes "software" designed to destroy, damage, degrade or disrupt systems, equipment or "software", specified by the Munitions List, cyber reconnaissance and cyber command and control "software", therefor'. Thus, the Wassenaar Arrangement applies to 'cyberweapons', used in a *purely* military manner. However, 'Pegasus' and the like are not designed to 'destroy, damage, degrade or disrupt' military systems. Instead, they intrude and manipulate civilian cell phones.

But software often has both, military *and* civilian use. Generally, the Dual-Use List covers such dual-use items, including dual-use software. However, it does *not* directly cover any dual-use items that can be classified as 'cyberweapons'. Instead, the Dual-Use List only names items *related* to intrusion software: Specifically, 'systems, equipment, and components' (Cat. 4.A.5 Dual-Use List) or 'software' (Cat. 4.D.4 Dual-Use List) 'specially designed or modified for the generation, command and control, or delivery of "intrusion software"'. The Wassenaar Arrangement defines intrusion software — and, therefore, arguably a type of 'cyberweapon' — in its definitions section. According to the definition, intrusion software is '"[s]oftware" specially designed or modified to avoid detection by "monitoring tools", or to defeat "protective countermeasures", of a computer or network-capable device' and to perform either 'extraction

of data' or 'modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.' Thus, the Arrangement does not place intrusion software *itself* on the Dual-Use List but only related items.

The Arrangement, therefore, applies only to 'Pegasus'-related exports. As intrusion software, 'Pegasus' itself is not among the listed items. But supplying the necessary IT infrastructure to employ and control 'Pegasus', retrieve data, and provide technical assistance (Cat. 4.E.1.c Dual-Use List) to other States, which NSO certainly did, requires prior licensing. Indeed, the Israeli government approved each export of 'Pegasus'-related technology. Crucially, however, the underlying decision of whether a specific export of 'Pegasus' is compatible with the goals and aims of the Arrangement and, therefore, eligible for a license remains within the sole discretion of Israel. Something the Israeli government apparently answered in the affirmative. Thus, Israel acted within the bounds of the Wassenaar Arrangement, thereby confirming its authority. However, this conclusion lays bare the lack of a mutual understanding within the Arrangement which circumstances necessitate the denial of an export license.

The Way Forward

In line with the aforementioned, the Wassenaar Arrangement applies to offensive military 'cyberweapons' and items related to intrusion software like 'Pegasus'. It, therefore, draws a baseline in the non-proliferation efforts against 'cyberweapons'. However, it does not offer an entirely comprehensive export control regime for 'cyberweapons': Its limited membership and the categories of 'cyberweapons' on the Dual-Use List would have to be broadened to close existing gaps. Moreover, although the Arrangement's non-binding character does not necessarily render it ineffective, a strengthened compliance mechanism would boost its effectiveness. Finally, participating States should try to find common ground on the circumstances under which an export license should be denied.

In addition to *international export control law,* other areas of international law, as well as supranational and national law, might offer an extra layer of protection against the irresponsible proliferation of 'cyberweapons'. This includes above all positive and due diligence obligations derived from international human rights, as well as the recently recast EU Dual-Use Regulation, which expressly addresses 'cyber-surveillance items' and transforms the non-binding Wassenaar Arrangement's lists into binding European law. Moreover, the efforts to regulate the proliferation of 'cyberweapons' should not preclude the ongoing efforts to promote responsible state behavior in cyberspace and regulate the *use* of 'cyberweapons'.

Even with an effective export control regime in place, the nature of 'cyberweapons' and their intangible transfer make enforcement challenging. An unsatisfied NSO employee, for example, copied the source code of 'Pegasus' and offered it in the darknet (see here). Thus, the answer to the risks posed by 'cyberweapons' must go further than banning or controlling their export. The promise of a secure and stable 'cyberspace' can only be achieved if the core of most 'cyberweapons' is terminated: (zero-day) vulnerabilities. Consequently, States need to promote adequate, international zero-day vulnerabilities governance, including the responsible disclosure of such vulnerabilities, instead of hoarding them.

Cite as
Roland Klein Trimming Pegasus' Wings: International Export Control Law and 'Cyberweapons', Völkerrechtsblog, 27.10.2021.