On spyware and its use by US intelligence services

The improvement of information encryption algorithms forces interested entities (intelligence agencies, criminal and terrorist organizations, etc.) to seek new opportunities to gain access to information they are interested in. One of such methods is to gain control over mobile devices by exploiting previously unknown vulnerabilities (the so-called zero-day vulnerabilities), which enables to extract data before it is encrypted.

The number of commercial companies developing appropriate software is constantly growing. The most famous of them are NSO, Paragon, Intellexa (all three are Israeli) and Bolden (US). The products offered by them have different functionality. The abovementioned American company provides tools for hacking WhatsApp messenger. Software Pegasus, Phantom (by NSO) and Predator (by Intellexa) allow obtaining any information from the cellphone memory. The Graphite software package (by Paragon) enables additional data extraction from cloud storage after backup from a device (for this reason, it becomes even more difficult to detect traces of spyware penetration). The software can be injected into cellphones remotely without the owners’ knowledge (Pegasus, Phantom, Graphite) or after clicking a specially sent infected Internet links (Predator).

The extensive covert surveillance capabilities of these software products have obviously attracted the attention of the United States, which is interested in continuously improving its global NSA-based electronic espionage system. Relevant software is purchased and widely used by intelligence services. For example, in 2018, the CIA bought a license for Pegasus under the pretext of assisting the Government of Djibouti in countering terrorism. In 2019-2021, the program was actively used by the FBI. As key vulnerabilities were eliminated by mobile device manufacturers and, consequently, the effectiveness of Pegasus decreased, the Americans switched to Graphite software. According to available information, this program is used by the U.S. Drug Enforcement Administration
(DEA) allegedly for operations outside the country alone (and not against American citizens).

It is demonstrative that Washington tried to dissociate itself the use of Pegasus amid a wave of media revelations about the use of the program against journalists and politicians around the world. In 2021, NSO was even blacklisted by the US Department of Commerce for actions that undermine national security and contradict the country’s foreign policy interests. Moreover, in the new edition of the National Security Strategy released in October 2022, the US administration was forced to make a formal commitment to counteract the “unlawful use of technology, including commercial spyware”. At the same time, all inquiries to the DEA regarding the use of Graphite remain unanswered.

The US continues to use surveillance programs uncontrollably and encourages their development, using them as a foreign policy tool for its own narrow selfish purposes. This is another evidence of the “double standards” policy: while defending the notorious “democratic values” at the international arena, in practice, Washington openly neglects the protection of human rights and fundamental freedoms, the UN Charter and the fundamental international legal principles of sovereign equality and non-interference in the internal affairs of States.

Shaping fair international legal mechanisms for regulating information space can be an effective tool to counter such a policy. This implies, primarily, developing legally binding agreements that would take into account the specifics of ICTs (anonymity, crossborder nature, technical vulnerabilities, constantly improving software and hardware capabilities) and would ensure their use for peaceful purposes only. Active efforts in this area are being made under the auspices of the United Nations within the framework of negotiating platforms established upon the initiative of Russia – in the Open-ended Working Group on International Information Security and the Ad Hoc Committee on the Elaboration of a Comprehensive Convention on Countering the Use of ICTs for Criminal Purposes.