The Hebrew University's Harrry and Michael Sacher Institute for Legislative Research and Comparative Law, and the Hukim Journal on Legislation: Roundtable Discussion on Law and Cyberspace

Hacking in the Fight Against Terrorism: Israeli, Comparative, and International Perspectives

Asaf Lubin[1]

The Counter-Terrorism Bill, 5775-2015, introduced an array of criminal law and public law tools aimed at assisting the State of Israel in effectively fighting against terrorism. Simultaneously, the Bill sought to ensure a balance between the security interests, enumerated therein, and Israel's commitments to "human rights and to customary international legal standards". Of the various tools introduced in the Bill, Section 131 was one of the most controversial, as it called to amend the General Security Service Law, 5762-2002, and provide the Shabak with statutory authorization to engage in hacking of electronic devices for the purposes of preventing acts of terrorism and espionage directed against the State. The Bill's commentary clarifies that with the rise in terrorist activity which relies on advanced computerized technologies, there is a "vital need" in expressly authorizing the Shabak to employ such cyber techniques that would allow it to break into digital devices and computer networks. On 28 March 2016 the Constitution, Law and Justice Committee of the Knesset voted to split Section 131 from the Bill. As a result, the Counter-Terrorism Law, which passed its third reading this past June, avoided dealing with the question of the authority of Israeli law enforcement and intelligence agencies to engage in investigative techniques in cyberspace. As of now, the Committee has yet to hold a session on the now separated Section 131, but it remains on the agenda for the remainder of 2017.

Under Section 23A of the Criminal Law Procedure Ordinance (Arrest and Search), 5729-1969, any access to "materials on a computer system" (as the term is defined under the Computers Law, 5755-1995) constitutes a search. Accordingly, all covert hacking activity taken by Israeli authorities is subject to the issuance of a warrant by a magistrate or district judge that would specifically authorize such access, and lay out its parameters and its objectives. Section 131 proposes to ease the Shabak's ability to engage in hacking for coutner-espionage and counter-terrorism purposes, by sidestepping the acquisition of a Court issued warrant. Under the proposed amendment the Prime Minister, at the request of the head of the Shabak, could directly authorize such hacking, if he was convinced that "the operation was vital for the purposes of preventing or obstructing terrorist activity or espionage, that could potentially endanger human life, or cause significant harm to Israel's security, and that no other means are reasonably available to achieve the aim sought". The proposal further states that in urgent cases, the Head of the Shabak could himself authorize such hacking, subject only to an immediate notification to the Prime Minister Office. Section 131 establishes two mechanisms which are seek to ensure "careful and proportionate" use of the stated authority: First, the proposal establishes temporal limitations on the duration of these authorizations (30 days for an authorization issued by the Prime Minsiter, and 48 hours for an authorization issued by the Head of the Shabak); Second, the proposal establishes that insofar as the targeted device is in use by a lawyer, doctor, psychologist, social worker, or a member of the clergy, a court warrant must still be acquired prior to engaging in such hacking (with the caveat of urgent matters, in which case the Prime Minister may be allowed to authorize the hack subject to a reporting to the Attorney General, who in turn will have the power to revoke the authorization). In essence, Section 131 attempts to duplicate the legal framework that exists for wiretapping for national

[1] J.S.D Candidate, Yale Law School (18' expected); Visiting Fellow, Information Society Project; 2016-2017 Robert L. Bernstein International Human Rights Fellow, Privacy International.

security purposes, under the Eavesdropping Law, 5729-1979, and apply it, *mutatis mutandis*, to hacking operations.

The desire of the Israeli legislator to expressly regulate the authorities of the Shabak in cyberspace, reflect a growing trend amongst western democracies to establish, through primary legislation, effective frameworks that could control the use of hacking powers by intelligence agencies and law enforcement, in the prevention of serious crime, namely the crime of terrorism. If, in the past, operations such as these were subject to confidential internal administrative guidelines and regulations, the calls for transparency and accountability in the age of Edward Snowden and WikiLeaks, have brought with them a rise in statutory authorizations. In the Untied States, for example, Congress adopted, this past December, an amendment to rule 41 of the Federal Rules of Criminal Procedure. This amendment grants a magistrate judge the power to issue a warrant to use "remote access to search electronic storage media and to seize or copy electronically stored information" even in cases where the location of the targeted devices is unknown to law enforcement (as it is concealed through anonymizing technologies, such as TOR). The judge is in essence authorized to issue warrants that would be enforced outside of his or her district, indeed potentially outside of the country. Also in December, the United Kingdom adopted the Investigatory Powers Act which grants the Home Secretary the authority to issue "equipment interference warrants" both within and outside the United Kingdom. Moreover, the Act authorizes the Secretary to issue bulk warrants, that is the hacking of devices of a group of individuals who share similar characteristics, and not only the devices of a particular suspect, for whom there is reasonable suspicion. Similar legislation has been adopted in recent months and years in Italy, the Netherlands, Germany, and France.

In this Article, I wish to compare the amendments listed in Section 131 with similar legislation around the world. Moreover, I wish to examine the extent to which the amendments are line with the international obligations of Israel, including in particular the customary rules surrounding the right to privacy under international human rights law. For this purpose, I will review the surveillance jurisprudence and commentary of the Human Rights Committee and the regional human rights Courts. The discussion surrounding Section 131 opens a narrow opening for a conversation, often lacking in Israeli discourse, as to the nature and scope of operations by the Israeli intelligence community, and the checks and balances on their purported activities. As part of the research of this paper I would seek to answer the following questions: (1) To what extent should the law limit, through primary legislation, the discretion of law enforcement and intelligence agencies in engaging in hacking activities (and in this regard, would different types of hacking operations yield different answers)? (2) What are the categories of offences for which hacking operations should be authorized; (3) What *ex ante* and *ex post* oversight mechanisms and minimization procedures should be introduced to ensure that every hacking operation meets standards of legality, necessity, and proportionality; (4) To what extent should transboundary hacking be authorized through primary legislation; (5) What notification requirements apply to the authorities engaging in such hacking activities, and how to ensure the right to access to justice and remedy of the potential victims of arbitrary hacking and abuses of power?