Outcomes of the Workshop on "The Challenges of Cybersecurity Legislation: On the New Draft Cybersecurity Law"

On Sunday, November 20, 2018 the Center held a jointly-sponsored Workshop for Israeli and international experts on the draft Cyber Security and National Cyber Directorate Bill published by the Prime Minister's Office on June 20, 2018.[1] The workshop was held at the Israel Democracy Institute, with the cooperation of that Institute, the National Cyber Directorate (NCD), and the the Israel Tech Policy Institute. Participants included cyber and regulatory experts from Israel, the US, the EU, and the OECD.

Many of the issues raised during the discussions shed light on areas that have sparked public attention and concerns following the publication of the bill. In particular, the workshop focused attention on the proposals raised by academics, private sector actors, and international cyber experts to amend the draft bill in order to include additional critical checks and balances to the draft bill. The timing of the Workshop coincides with the current drafting stage: the preparation of the draft bill for government approval in view of the comments received, including a submission by the Cyber Security Research Center[2] and the Israel Democracy Institute.

The bill establishes the INCD as Israel's national cybersecurity authority, bolstering its role in assessing national cyber risks, planning for national preparedness and resilience, establishing information sharing mechanisms, and providing guidance to both government agencies and the Israeli private sector. However, the current draft has provoked controversy due to its treatment of a number of key issues, including what has been described by some commentators as "extensive powers" for cybersecurity incident response or attack mitigation, such as powers to request documents and computer data from private sector organizations to identify and mitigate cyber attacks, and to seize equipment for analysis for these ends. Some of these activities, such as access to computer networks, require judicial authorization under the bill. Nonetheless, the requirement for *ex ante* judicial authorization may be waived under certain extreme conditions that justify urgent action in the view of the Head of the INCD. The INCD is required to report

[1] See the original Hebrew draft bill at http://www.tazkirim.gov.il/Tazkirim_Attachments/44319_x_AttachFile.docx (Hebrew); as well as two commentaries in English: Amir Cahane, The New Israeli Cyber Draft Bill – A Preliminary Overview, <https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill>; and Deborah Housen-Couriel, A Look at Israel's New Draft Cybersecurity Law, https://csrcl.huji.ac.il/people/look-israels-new-draft-cybersecurity-law-new-draft-cybersecurity-law?ref_tid=3718.

[2] The Cyber Security Research Center notes on the new Israeli Cyber bill (Hebrew) (11.7.2018) <https://csrcl.huji.ac.il/sites/default/files/csrcl/files/tzkyr_khvq_hsyybr_-_hrvt_mrkz_hsyybr_20180711.pdf> .

such an urgent use of power to the Attorney General and to apply for an authorizing warrant within six hours. Public commentary around the draft bill has focused on the scope of powers it accords to the INCD, both procedurally and substantively, as well as on the degree of transparency regarding the INCD's proposed authorities.

The Workshop was opened by Professor Yuval Shany, who characterized the draft bill as an important effort to set "the rules of the game" of cybersecurity in Israel's civilian sphere, including the difficult balances needed in a democracy between national security concerns and individual freedoms. In Professor Shany's view, the apparent ease with which government surveillance can be conducted in cyberspace – as demonstrated by the Snowden disclosures of NSA surveillance in 2013 – raises particular challenges for setting boundaries for government access to computer data and oversight mechanisms.

The first presentation was made by Yigal Unna, Director-General of the INCD, who addressed the institutional mandate of the INCD as it has evolved since its inception in August of 2011. He emphasized that in Israel, as elsewhere, the legal and regulatory frameworks that apply to cybersecurity are struggling to catch up with operational needs. Unna described the four major vectors that influence security challenges and operational needs: (a) new technological capabilities that are constantly evolving and create "asymmetry" in cyber threats, (b) the advancement of computing capabilities, including "adversarial AI," (c) geopolitical challenges and threats, and (d) the undermining and erosion of trust in governmental authority in cyber-targeted countries. Operationally and internally, the INCD aims for a clear division of responsibilities for carrying out its mandate of building a robust cyber domain, detection and mitigation of cyber threats to Israel, and of developing national resilience when attacks do occur.

The first panel provided the participants with an overview of various cybersecurity legal regimes. It began with an outline of the OECD Digital Policy,[3] which emphasizes the social and economic aspects of the cybersecurity challenge. Noting that under current societal trends, digital services are becoming more and more essential to the functioning of a hyper-connected society, digital security should be viewed as an important form of risk management for essential

[3] DIGITAL SECURITY RISK MANAGEMENT FOR ECONOMIC AND SOCIAL PROSPERITY: OECD RECOMMENDATION AND COMPANION DOCUMENT (2015) <http://www.oecd.org/governance/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm>

societal functions. Having acknowledged the impossibility of eliminating all threats, we should aim to reduce them to an acceptable level to the national economy and societal functions. Governments should adopt a coherent approach to digital security risks encompassing all stakeholders, as the threats cannot be reduced by a single actor. Therefore, results are to be based on long term private-private, private-public, and public-public cooperation. In order to facilitate such cooperation, the governance must foster long-term trust, while also respecting human rights and fundamental values.

The newly-established US Cybersecurity and Infrastructure Security Agency (CISA) was presented to the Workshop as different in its approach from Israel and many European countries. CISA operates under a voluntary framework, based on cooperation from private sector entities on a consensual and non-coercive basis. A key factor in creating trust with the private sector are CISA's obligations to protect information, facilitating cooperation by providing assurances that information will not be shared with other agencies or used for regulatory purposes. CISA also offers proactive services to private companies to assess the robustness of their security.

Next, the Workshop was presented with an overview of the cybersecurity regulatory framework in Germany. The mission statement of the German cybersecurity agency, the BSI, is threefold: prevention, detection, and reaction (to threats). Unlike other key players in the field (such as the Federal Criminal Police Office (BKA), the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND), and the Military Counterintelligence Service (MAD)), the BSI is not vested with any police or intelligence-related powers. However, the BSI has several legal measures to protect cybersecurity. These include powers to monitor all federal communications (i.e., government communications),[4] to operate mobile incident response teams (MRTs) subject to the respective party's request,[5] to issue public warnings regarding malware or security failures (subject to preliminary

[4] See Act on the Federal Office for Information Security (BSI Act – BSIG), Sec.5. English translation available on <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf;jsessionid=83ECBFA46D09BC550E480D81259DA95C.1_cid369?__blob=publicationFile&v=4>

[5] BSIG, Sec. 5a.

notification of the relevant parties),[6] and to reverse engineer and examine IT products and hardware for security risks.[7]

The cybersecurity agency of the Netherlands, the National Cyber Security Centrum (NCSC), was also briefly reviewed. The NCSC has no legislative function, nor is it vested with any supervisory or enforcement powers. It serves as an information hub, gaining trust from the private sector by having restrictions on information sharing with other government departments. Although not applicable to the NCSC directly, the Dutch intelligence oversight framework was also outlined,[8] in view of its possible contribution to the discussion of controls and safeguards mechanisms in the context of the Israeli draft bill.

The second panel of the day focused on dilemmas and issues arising from the intersection between cybersecurity and privacy. Acknowledging the necessity of cybersecurity, the seriousness of the threats and cybersecurity's core role in protecting privacy (as many privacy issues have been implicated by data breaches), participants raised concerns regarding aspects of the Israeli draft bill, which may endanger privacy rights and civil liberties.

Central to these concerns is the proposal in the draft bill to create an early warning information sharing system based on the monitoring of the networks of sensitive high-profile organizations. While acknowledging that the aim of the early warning system is to share information about cyber attacks and detect them at an early stage (such as in the case of spreading epediams), some participants were concerned about misuse of the system for surveillance of human activity. In case of such misuse, participants were concerned of the possible chilling effects caused by such a surveillance apparatus. Such misuse may indeed lead to chilling effects and encourage self-censorship, eventually leading to difficulties in facilitating political changes, as there might be reduced free sphere for the exchange and development of ideas. On the other hand, the INCD representatives pointed out that the protection of the cyber ecosystem from adversary misuse is a more reasonable scenario, and that effective protection is thereby afforded to basic rights, including free speech and the exchange of ideas.

[6] BISG, Sec. 7.
[7] BISG, Sec. 7a.
[8] For an overview of the intelligence oversight system in the Netherlands, see Quirine Eijkman et al, "*Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017"* , IViR 2018 <https://www.ivir.nl/publicaties/download/Wiv_2017.pdf>

Concerns were raised that according to possible interpretations of the draft bill it may allow for the collection of personal identifiable information, which might over time facilitate mission and intelligence creep and the use of this information by other government agencies and authorities. Further comments were made as to the possible need to differentiate between the privacy standards relevant to each regulated sector (banking, insurance, health, etc.).

Additionally, it was noted that the proposed statutory purposes of the INCD under the draft bill includes "promoting Israel as a world leader in the cyber field".[9] Accordingly, certain invasive powers granted to INCD thereunder should be limited to cybersecurity purposes only. This comment was disputed by the INCD representatives, noting that the preliminary conditions for use of authorities under the draft bill are more granular, effectively limiting use of powers for issues not directly related to cyberattacks. The INCD is indeed charged with the role of promoting Israeli leadership in cyber, but this task does not require using the powers in the bill.

The need to strengthen the oversight framework for INCD activities was stressed. Certain concerns about the independence of the INCD internal privacy supervisor were mentioned, as was the need for a proper mechanism for resolving conflicts between the supervisor's direct superior, the head of the INCD (or a senior NCD officer whose direct superior is the head of NCD), and the supervisor's professional guidance from the Israeli Database Registrar (in the Israeli Data Protection Authority).[10]

Addressing the need to facilitate trust, participants suggested strengthening external supervisory frameworks, increasing transparency, and adding more general principles (such as a strict purpose limitation) to the draft bill or another piece of primary legislation. External oversight bodies should report not only to the Prime Minister, but also to a parliamentary committee. The proposed oversight committee mandate could be expanded beyond "privacy," and it should be required to meet regularly.

However, it was also noted that cybersecurity agencies are rarely interested in content. The nature of the data collected should be taken into account while reviewing the privacy framework suggested in the draft bill. Overburdening government agencies due to misplaced

[9] NCD draft bill, Sec. 2(b), 3(3).
[10] NCD draft bill, Sec. 10(d).

privacy concerns may impede them from serving their purpose. Privacy by design may provide reassurance for most of these concerns.

The Workshop concluded with a summary of the key issues and discussion of new questions, moderated by Dr. Tehilla Shwartz Altshuler.

Dr. Shwartz Altshuler noted the ambiguous definition of "information of security value,"[11] compared to possible alternatives, wondering whether such a broad definition is necessary, and whether such information could be further misused to profile and regulate individual behavior.

Professor Lokke Moerel mentioned the need to design proper checks and balances, safeguards, and boundaries in order to address possible abuses of power, in light of the authorities proposed. Professor Tal Zarsky doubted the effectiveness of the privacy committee proposed in the draft bill, suggesting instead the inclusion of sunset clauses in the law, enabling periodic legislative review. Assuming substantial future developments in the cybersecurity field, within a decade it may prove necessary to undertake a fundamental revision of significant parts of the law.

Professor Yuval Shany described the draft bill as a direct continuation of the legal framework enabling online surveillance in Israel. In his view, these offer broad intrusive powers with weak safeguards. As the draft bill goes beyond purposes of addressing "security threats," it would be unfortunate to apply the deficient online surveillance model, comprising weak and non-transparent safeguards, in the world of cybersecurity.

The participants also debated whether the INCD should be compared with other government agencies, regulators or with the Israel Security Agency (the secret service) when discussing the safeguards applicable to data collection powers and coercive powers under the draft bill. Relating to the concerns raised regarding abuse of power, Amit Ashkenazi, the legal advisor of the INCD, stated that Israel's administrative tradition and application of administrative law principles such as purpose limitation, reasonableness, and proportionality serve as a substantial general limitation on the misuse of power and on possible intervention by the Prime Minister. He noted that several security organizations are in the Prime Minister's Office but that does not entail the ability to corrupt them, due to external governmental and internal controls.

[11] NCD draft bill, Sec. 1.

A second point made by Dr. Shwartz Altshuler was the regulatory approach in the draft bill, which sets in place an overarching regulator, regulating already existing sector-specific regulators. She cautioned against unwillingness of regulators to cooperate with INCD guidance. However, both Gabriel Taran and Laurent Bernat noted that "regulatory greed" (i.e. a push towards expansion of bureaucratic competencies) is not a unique Israeli phenomenon and suggested that an agency with overarching powers may be a good approach to handling such a policy issue crossing many sectors.

Advocate Ashkenazi observed that there are benefits to the meta-regulatory model, and he did not share many of Dr Shwartz's concerns. In his view, as a result of the required cooperation between INCD and the sector specific regulators, the possible tensions and frictions need to be resolved within government, and not by issuing conflicting directives to the private sector.

Dr. Shwartz Altshuler also raised concerns about a possible future expansion of the INCD's missions by regarding cyber operations that target content or "fake news" as cyber threats to be dealt with by the directorate, under the general vague mission of "maintaining trust in democratic institutions."

Concluding the workshop, she referred to one of INCD's primary goals as proposed in the draft bill, which is the advancement of Israel as a leader of cybersecurity, saying that in a small country such as Israel we will not be leaders of cybersecurity without simultaneously protecting fundamental human rights.