



Report of the State Comptroller of Israel | May 2022

Systemic Topics

The Law Enforcement System's Treatment of Cybercrime



The Law Enforcement System's Treatment of Cybercrime

Background

Over the last decade, the use of the Internet has increased: computers, smartphones, and other technological tools based on the use of the Internet have become, both in Israel and around the world, the main tools for work and communication and the primary means of entertainment during leisure time. They store a great deal of information including, personal details and memories, economic, industrial, public and governmental information. The accessibility of cyberspace and its unique characteristics, including anonymity, the volatility of evidence, the decentralization of information, supra-territorial encryption capabilities, automation, and low usage costs and accessibility to an unlimited number of victims in a short time, have increased the scope of crime and terrorism in this space and have become fertile and accessible grounds for criminal offenses. Numerous crime areas have moved to this space, and new threats have even emerged therein, challenging the law enforcement systems. All of these expose the technological tools and the Internet users to a variety of possible vulnerabilities and dangers, including among other things, crimes against minors, crimes of fraud and theft of information and money, illicit trade in weapons and drugs, attacks on computers and communication networks and preventing access to it, and inciting violence and hate crimes (crime in the cyberspace or cybercrime). In recent years, the Israel Police has declared dealing with cybercrime as an organizational goal of the utmost importance, given the emerging changes in the world of crime and the apparent trend of crime transitioning to cyberspace.

This audit mainly deals with the Police's preparedness to cope with cybercrime and with criminals exploiting cyberspace to harm organizations and individuals; however this report does not deal with the Police's use of technological tools as part of its overall intelligence and investigative activities in respect of all the areas of enforcement it carries out¹.

It should be noted that the principle underlying this audit is the duty of the Police to use the tools, means, and equipment at its disposal only according to the provisions of the authorizing legislation, orders, and procedures and to act by the specific instructions it receives from the legal counsel in the various cases. In this context, the Police must take care that the fight against cyber criminals and the exercise of its powers in the areas of intelligence and investigation will be conducted in ways that may not harm the fundamental rights of the individual and his privacy, unlawfully.

1 An audit on this subject is planned for the next working year.



Key figures

**about USD
6 trillion**

the estimated amount of cumulative damage caused by cybercrime worldwide in 2020, and it is expected to increase every year, up to USD 10.5 trillion in 2025

**about
87%**

victims of crimes in cyberspace in Israel in 2019 (about 200,000 people) did not report the crimes committed against them to the Police, according to the survey of the Central Bureau of Statistics (CBS)

**about
250%**

the increased rate of investigation cases in the Police regarding cybercrime in the years 2016–2020 (from 2,506 to 8,821 cases)

**about
75%**

of the cases investigated by the Police concerning cybercrime in 2018–2020 were closed (19,253 out of 25,707 cases), and in about 63% of them, the reason for the closing was "Unknown Perpetrator"

**in about
90%**

of the investigation cases opened in 2018–2020 on cybercrime, no indictments have been filed

53%

the rate of cases opened at the State Attorney's Office that dealt with economic crime (money laundering, fraud, and selling stolen credit card details)

**304
million**

the number of ransomware events around the world in 2020

**about NIS
350
million**

the Israel Police assesses the total budget required for establishing an information fusion system in the Police, for comprehensive technological equipping, and for employing professional cyber consultants. This budget has not yet been allocated

Audit actions



From March to August 2021, the State Comptroller's Office examined the law enforcement system's handling of cybercrime, including the normative regulation of the fight in this crime arena and the professional training of the designated officials. The




examination was conducted at the Police headquarters, the National Cyber Unit in Lahav 433, and at the cyber divisions in the Police districts. Completion examinations were conducted in the National Cyber Unit at the State Attorney's Office and the Legal Counsel and Legislative Affairs Department at the Ministry of Justice, the Ministry of Public Security, and the National Cyber Directorate. As part of the examination, the State Comptroller's Office monitored the previous audit recommendations implementation – "The Israel Police's Treatment of Sophisticated Cybercrime"² published in 2017.


This report was presented to the Prime Minister and the State Audit Committee of the Knesset on February 15, 2022, and was classified as confidential until the State Audit Committee's subcommittee hearing.

By the authority under Section 17(c) of the State Comptroller Law, 1958 [Consolidated Version], and after considering the government's arguments, consulting with the bodies responsible for the protection of national security information and in coordination with the Chairman of the Knesset, since the subcommittee above did not convene, it was decided to publish this report while imposing confidentiality on sections of it. These sections shall not be submitted to the Knesset, nor shall they be published.

The findings of the audit report and its recommendations are valid as of the date of its presentation.








Key findings

 **Coping with ransomware crimes** – despite the 150% increase in the scope of ransomware crimes around the world, which was estimated in 2020 at approximately USD 20 billion, and the heavy economic damage caused to the Israeli economy, estimated as mentioned in the hundreds of millions of NIS, it was found that the Police has not formulated a plan to deal with this unique crime phenomenon.

 **Citizens' satisfaction with the Police's handling of cybercrime** – about half of the victims of crimes in the cyberspace who reported it to the Police, claimed in the 2019 CBS survey that they were not satisfied with the Police's handling, and 84% of them expressed their dissatisfaction with its approach. In the 2020 CBS survey, 51% of the participants responded that should they be affected by cybercrime, they would report it to bodies outside the Police or not report it at all.

² The State Comptroller, **Annual Report 67B** (2017), p. 1851.



-  **The activities of the National Cyber Center** – the National Cyber Center (NCC) in Lahav 433 operates without a detailed methodology and appropriate technological equipment. The staffing at the NCC is mainly based on high turnover personnel: two police officers, two students, and five volunteers in national service.
-  **The Internet as a space without control and protection** – the Police intelligence situation report for 2020 raised that the Internet is a space over which the state has no control, and thus it fails to protect its security and economic interests and those of its residents, including in the aspect of personal safety and privacy.
-  **Gaps in cooperation with security agencies and the National Cyber Directorate** – although there is an intelligence and operational need to institutionalize cooperation between the Police and defense system bodies, with an emphasis on the intelligence community, there are no fixed working mutual mechanisms between them.
-  **Closing investigation cases involving cybercrimes** – more than 25% of the 36,009 cases opened by the police in the years 2018–2020 and classified as "internet-related" were closed outright; 75% of the remaining investigation cases were closed, most of them (about 63%) on the grounds of "Unknown Perpetrator" (when the person who committed the crime was not found or when there is no suspicion as to their identity); The handling of these investigation cases was brief, up to ten days, and most of the cases were closed in less than a month.
-  **Coping with complex digital attacks** – the professional knowledge currently available in the Police is mainly used to investigate simple criminal cases, particularly phishing attacks, and sexual blackmail online. Still, insufficiencies have arisen regarding the ability of investigators to cope with specific digital attacks.
-  **Lack of means of attack and thwarting cybercrime** – there is a significant lack of basic and advanced equipment in the cyber and technological units, which does not comply with the Police procurement plans for 2019–2020. The lack of said means impairs the ability to gather intelligence and the means of attack for thwarting cybercrime, making it difficult for investigators to locate criminal activity in cyberspace and track it down. Hence, the cyber and technological units find it difficult to exhaust digital evidence in all incidents in the absence of technological means.
-  **The activity of the Cyber Unit in the State Attorney's Office on the voluntary enforcement level** – the action of the State Attorney's Office on the voluntary enforcement level (according to which it turns to the operators of websites containing illegal content to remove it) is done without explicit authorization by law, but by the government's residual authority and the auxiliary powers of the Attorney General. The State Attorney's Office acts at the request of an injured public servant or an authorized party with the employee's consent but does not act in favour of the general public victims. In a High Court of Justice ruling published in April 2021, it was recommended



that the State Attorney's Office consider a regulating and detailed legislative initiative regarding the entirety of voluntary enforcement, as is done in some Western countries.



The activity of the Courts Administration to remove publications against judges – commencing in 2015, the Courts Administration initiated an independent voluntary enforcement to remove publications against judges. In 2016, the Courts Administration made 97 requests to website operators, which gradually decreased until in 2019, 3 requests were made, and in 2020 no requests were made. This activity, which was not explicitly included in the framework of the administrative authority granted by the Courts Law to the Director of the Courts, was anchored in an internal procedure that was updated in December 2019 with the approval of the Attorney General.



The legal regulation of the fight against cybercrime – there are accumulated gaps over the years due to the need for regulation and legislative amendments in the enforcement field against cybercrime, which has not yet been updated. The existing legislation does not provide a complete and practical response to cyber threats and is not adapted to rapid technological development. These findings illustrate the need to provide effective tools to law enforcement bodies in their activity against crime and an up-to-date legal regulation of its powers.



NCC operates all year round, 24 hours daily; it functions as a national body and serves all enforcement and security systems. The State Comptroller's Office commends NCC's activities, despite the lack of skilled personnel and appropriate technological means.

Key recommendations



It is recommended that the Sigint-Cyber Division in the Investigations and Intelligence Division, which is in charge of building the force and its operational concept, promote an outline for the positioning of the NCC in the police cyber system, which will include a detailed regulation of its roles, its work methodology, and of the human and material resources, it requires. This is within the framework of the provisions of its authorizing legislation, orders, and procedures.



It is recommended that the Police formulate an up-to-date operating concept, including: updating the existing organizational structure; regulating the infrastructure for the activity of all the intelligence, investigations, and operations bodies in the police cyber system, with an emphasis on the technological aspect; characterizing the work mutual mechanisms between the police bodies and establishing the required collaborations



between them and the relevant bodies in the governmental space and the international arena.



The Police should incorporate the lessons emerging from the intelligence situation report into its work plans, to reduce the substantial intelligence information gathering gaps regarding crimes in cyberspace.



It is recommended that the Standing Committee³ implement its joint team's recommendations regarding strengthening inter-organizational cooperation, including enforcement and security bodies. These will help the Police to improve their abilities in gathering intelligence information, acquiring professional knowledge and technological skills, to improve the investigation means of solving crimes and locating suspects in criminal incidents in cyberspace.



It is recommended that the Ministry of Justice promote the regulation of the voluntary activity of the Cyber Unit in the State Attorney's Office, examine ways to provide equal protection from cybercrime to all public employees, and consider responding to victims from the general public vis-à-vis the capabilities and resources required. It is also recommended that the State Attorney's Office consider making voluntary enforcement services available to the general public, noting that the documentation of the proceedings will be transparent to the public and that the necessary prioritization will be done according to the tools and resources at its disposal.



It is recommended that the Ministry of Justice, in cooperation with all the relevant bodies, promote the necessary amendments to the existing legislation on investigating crimes and gathering evidence in the technological arena and cyberspace; while examining their impact on the entirety of the public's rights, through a balance between the needs of the law enforcement system and the rights granted to the individual by law.

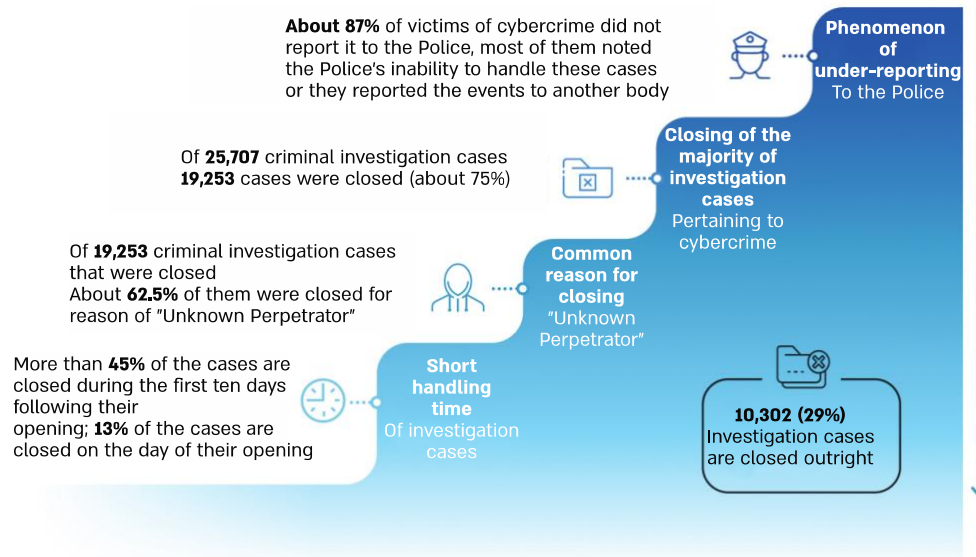


It is recommended that the Police examine how to close the gaps regarding the expertise required in the cyber fields for carrying out intelligence missions, investigations, and operations within the treatment of cybercrime.

3 A permanent inter-organizational committee for the direction and coordination of the activity in the fight against serious and organized crime and their products.



Summary of Findings Regarding the Police Handling of Cybercrime Cases





Summary

In recent years, there has been a steep increase of hundreds of percent in the scope of crimes in cyberspace in Israel and in the world, including crimes using computer programs that use advanced technology to commit crimes in physical space. Cybercrime endangers the individual, the general public, the state, global commerce, and even state security; It may threaten human life and the safety of women, men, and children, harming their property and privacy. In 2020, the total damage of cybercrime worldwide was estimated at about USD 6 trillion, which is expected to increase yearly. The challenges are complex and require, among other things, continuous cooperation between countries and between international organizations operating in this field.

In Israel, the Police is the primary body responsible to treat cybercrime. The findings in this report demonstrate that an up-to-date operating concept does not support the existing setup in the Police; does not include skilled personnel in the cyber professions to the extent required for the needs; and is not equipped with the technological means necessary to carry out its work in its entirety. According to data from 2019, there is a phenomenon of under-reporting to the Police of victims of cybercrime.

The estimates regarding a significant increase in cybercrime in the coming years require the enforcement bodies to increase their preparedness to guarantee the necessary enforcement response. It is appropriate that the Police concentrate effort both on building the force and on using it to combat cybercrime, with the support of the Ministry of Public Security and by the recommendations detailed in this report. Furthermore, the Police should ensure that any action taken with the technological means at its disposal, including hacking into private computer systems and cellular devices, will be done while protecting individual rights and by the necessary legal approvals.

The Attorney General's Office and the Courts Administration should regulate and authorize some of the enforcement actions they take. This regulation is required both due to balance the needs of the law enforcement system with the rights granted to the individual by law, and since the future foretells an increase in the incidents of cybercrime will require coordinated and planned action.