**תקציר הצעת מחקר: פשעי סייבר בבית הדין הפלילי הבינלאומי – המצוי והראוי**

**עדי ליבסקר-חזות**

**Cyber-crimes in the International Criminal Court: what is and what ought to be**

**Adi Libsker-Hazut**

In the decades that passed since World War II, significant developments have taken place in international law. The main developments are the establishment of the tribunals in Nuremberg and Tokyo, the Geneva Convention and its complementary protocols, and the establishment of the tribunal for the prosecution of war crimes in Yugoslavia and Rwanda. Very often, norms are applied retroactively in the prosecution of war criminals at those tribunals. As a result, the courts had to find various justifications for violating the principle of legality, namely, the imposition of criminal sanctions on acts that were not criminal at the time they were committed.

On July 17, 1998, at the end of a month of deliberations, 120 countries ratified the treaty of the International Criminal Court (also known as the "Rome Statute"). On July 1, 2002, following the UN resolution, the court's constitution came into force, and for the first time in the history of international law, the international community founded a permanent International Criminal Court.

Article 9 of the Constitution regulates a mechanism which shall determine the elements of crimes which may fall within the jurisdiction of the Court.[[1]](#footnote-1) In this way, the Rome Statute asks to fix the existing deficiencies in previous constitutions,[[2]](#footnote-2) since In Yugoslavia and Rwanda, there were no formal legal documents detailing the elements of crimes. Article 21(1)(a) of the Rome Statute puts 'elements of crime' at the top of the normative hierarchy alongside the rules of procedure, the rules of evidence, and the constitution itself. In September 2002, the Court published an appendix to the Constitution entitled "Elements of Crimes",[[3]](#footnote-3) which details, inter alia, definitions of acts which constitute an offense.

Recent developments in cyber warfare have led many experts to estimate that the use of cyber capabilities in war will increase in future conflicts. In recent years, many countries and organizations have demonstrated their capabilities in various conflicts. Cyber ​​warfare occupies a central place in the security budgets of many countries, and even in the fields of defense-related industry and commerce. These developments are not absent from academia, which develops various disciplines surrounding the subject. Ethics and law, as usual, lag behind the technological developments. Very little has been done in order to regulate the sphere of cyber-crimes at the state level. This is even truer with regard to international regulation, and particularly, with regard to the issue of war crimes in international law.

According to Jeremy Waldron:

 “It is a feature of the human predicament, not only of the legislator but of anyone who attempts to regulate some sphere of conduct by means of general rules, that he labours under one supreme handicap - the impossibility of foreseeing all possible combinations of circumstances that the future may bring […]”[[4]](#footnote-4).

Technological developments and capabilities, which are naturally kept under a heavy veil of secrecy until they are needed, emphasize the importance of Waldron's words. However, this is certainly not a justification for reliance on vague norms that harm the efficiency, certainty, and ascertain ability of the law.

In its first stage, the proposed study aims to examine the possible scenarios in which cyber warfare may constitute one of the four offenses within the jurisdiction of the International Court of Justice in Hague, in accordance with Article 5(1) of the Rome Statute:

The jurisdiction of the Court shall be limited to the most serious crimes of concern to the international community as a whole. The Court has jurisdiction in accordance with this Statute with respect to the following crimes:

(a) The crime of genocide;

(b) Crimes against humanity;

(c) War crimes;

(d) The crime of aggression.

In the second stage, I would like to examine and evaluate the current legal state of affairs in accordance with the 'elements of the crimes', including the interpretative possibilities that the Tribunal might face in dealing with cyber-crimes.

Finally, in the third stage, I would like to propose principles and rules that will disperse some of the legal ambiguity on the subject, and facilitate future dealings with cyber-crimes in international criminal law.

1. Knut Dormann, *Elements of War Crimes under the Rome Statute of the International Criminal Court: Sources and Commentary* (2003) p. 8. [↑](#footnote-ref-1)
2. William A. Schabas, *The International Criminal Court: A Commentary on the Rome* (2010) p. 386. [↑](#footnote-ref-2)
3. Preparatory Commission for the Int'l Criminal Court, Finalized Draft Text of the Elements of Crimes,U.N. Doc. PCNICC/2000/I/Add.2 (Nov. 2, 2000) (להלן: "Elements of Crimes"). ניתן לצפייה באתר: <http://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf>: “Pursuant to article 9, the following Elements of Crimes shall assist the Court in the interpretation and application of articles 6, 7 and 8, consistent with the Statute. The provisions of the Statute, including article 21 and the general principles set out in Part 3, are applicable to the Elements of Crimes” (שם בעמ' 1). [↑](#footnote-ref-3)
4. Jeremy Waldron, "Vagueness in Law and Language: Some Philosophical Issues", 82 *Cal. L. Rev.* (1994) 509, p. 537. [↑](#footnote-ref-4)