

TSCM & Cyber technical specification investigation.	Cyber & TSCM מפרט טכני
<p><b>A Technical Threat Analysis (TTA).</b>  A Technical Threat Analysis (TTA) that includes identification of parties who may wish to illegally eavesdrop on the site location in order to access confidential or information not available to the general public.</p>	<p><u>אנליזה של גורמי הסיכון.</u>  לימוד ובחינה של נקודות התורפה ודרכי הפעולות האפשרויות של התוקף, גיבוש תוכנית החקירה.  הערכות וביצוע הלכה למעשה.</p>
<p><b>RF investigation. (AUDIO&amp;VIDEO)</b>  In aim to locate and find transmitters in varieties mode such as:  VLF, LF, HF, VHF, UHF, SHF  In wide and variety method of modulation such as:  Analog (AM, FM, PM)  Digital (ASK, FSK, PSK, QSK, WIFI, GSM, 3G,4G, CDMA, Bluetooth)  Spread-spectrum and frequency-hopping.</p>	<p><u>חקירת RF (אודיו ווידאו).</u>  המטרה: איתור משדרים פעילים מסוגים שונים בתחום תדרים רחב מאוד DC-SHF) ובשיטות אפנון שונות.</p>
<p><b>RF VLF investigation.</b>  In aim to locate VLF transmitters.  Include electricity, telecommunication, and free wires.</p>	<p><u>חקירת RF בתחום VLF.</u>  המטרה: איתור משדרים פעילים בתחום שידורים VLF המתאים להעברת תמסורת על גבי כבלי החשמל והתקשורת.</p>
<p><b>RF ELF investigation</b>  In aim to locate sources of leakage of the magnetic field.</p>	<p><u>חקירת ELF.</u>  המטרה: איתור אמצעי TSCM לפי עוצמת השדה המגנטי.</p>
<p><b>Laser and IR investigation.</b>  From the site out from out in.</p>	<p><u>חקירת לייזר ואינפרא רד.</u>  המטרה: איתור משדרים פעילים בתחום פעולה זה.</p>
<p><b>AUX investigation.</b>  In aim to find any bypass telephones microphone,</p>	<p><u>חקירת ציוד קצה.</u>  המטרה: איתור שינוי באמצעים קיימים לטובת האזנה בחלל.</p>
<p><b>GSM 3G 4G 5G investigation.</b>  In aim to locate GSM transmitters in standby mode.</p>	<p><u>חקירת GSM 3G 4G 5G.</u>  המטרה: איתור משדרי GSM 3G 4G.</p>
<p><b>WIFI investigation.</b>  In aim to monitor and locate suspicious Devices and SSID &amp; interceptors.</p>	<p><u>חקירת WIFI.</u>  המטרה: איתור שימוש בתמסורת WIFI להעברת מידע. ובנוסף איתור מערכות תקיפה.</p>
<p><b>IOT investigation (Z wave + Zigbee).</b>  In order to understand the capabilities and features of the system, and locate suspicious devices.</p>	<p><u>חקירת IOT</u>  המטרה איתור מערכות "בית חכם" ותכונותיה להעברת מידע לצד ג'.</p>
<p><b>Ultrasonic investigation</b>  In aim to locate ultrasonic site "natural" leakage and ultrasonic attack transmitters.</p>	<p><u>חקירת אולטראסאונד.</u>  המטרה: איתור מערכות תמסורת אולטראסאונד (גלי קול בתדר הגבוהה מתדר השמע האנושי).</p>
<p><b>Bluetooth investigation</b>  In aim to locate Blue tooth suspicious devices &amp; interceptors.</p>	<p><u>חקירת Bluetooth</u>  המטרה: איתור משדרים הפועלים בשיטה זאת ובנוסף איתור מערכות תקיפה.</p>
<p><b>Physical investigation.</b>  In aim to locate threats such as: hidden tape recorders, hidden microphones (coil, optic, acoustic, fiber), hidden cam, hidden crossing wires, hidden Computerize collect info devices and others.</p>	<p><u>חקירה פיזית.</u>  המטרה: איתור אמצעי TSCM שאינם ניתנים לגילוי בדרך אחרת אלה בבדיקה פיזית.  ציוד עזר: מצלמה תרמית + NLJD</p>
<p><b>Producing Action report findings and recommendations.</b></p>	<p>הפקת דוח פעולה, ממצאים והמלצות</p>