

# האתגר החדש: משברים תקשורתיים בתחום הסייבר

## ירדן ותיקאי ויחיאל לימור

### מבוא

ביום שני, 24 בינואר 2022, אירעו ברחבי העולם כשבעים מיליון תקיפות, פריצות או ניסיונות פריצה למערכות ממוחשבות. זה לא היה יום מיוחד, והבחירה בו הייתה אקראית. בדיוק שנערכה לאחר יומיים העלתה כי ביום זה נעשו כשמונים מיליון תקיפות על מערכות ממוחשבות. כעבור יומיים נוספים התמונה חזרה על עצמה: כשבעים מיליון תקיפות.<sup>1</sup> חברת אבטחה בין-לאומית אחרת דיווחה כי בכל שנייה בתאריך אקראי בחודש פברואר 2022 התרחשו מאות תקיפות סייבר ברחבי העולם.<sup>2</sup>

לכל מתקפה יש יעד. ארגונים או מתקנים ממשלתיים וציבוריים, גופים עסקיים-כלכליים וחברות פרטיות. מי שהיה ראש לשכת החקירות הפדרלית בארצות הברית (FBI), רוברט מולר, טען בזמנו כי יש רק שני סוגים של חברות או ארגונים: אלה שכבר חוו מתקפת סייבר ואלה שעוד יחוו אותה.<sup>3</sup> כלומר, מתקפת סייבר אינה עוד שאלה של "האם", אלא של "מתי".

מתקפת סייבר עלולה לגרום לכך שהגוף המותקף ייקלע למצב של משבר, אם בגלל נזקים שנגרמו לו או מחשש לנזקים עתידיים ואם בגלל חשיפת חולשתו ופגיעותו. למשבר כזה, המכונה משבר סייבר, עשויים להיות פנים שונות.

לכאורה אין חידוש בעובדה שארגון נאלץ להתמודד עם משבר סייבר, שהרי כל ארגון, גדול קטן, עלול למצוא עצמו נאלץ להתמודד עם משבר. הטכנולוגיה המודרנית, שהפכה את הסייבר לכן בית ברחבי העולם, וההיקף הנרחב של מתקפות סייבר, יוצרים מציאות חדשה של "פן-סייבר-דמיה", לאמור מגפת סייבר כלל-עולמית. יתר על כן, משבר סייבר הוא רב-ממדי ויש לו היבטים שונים ומורכבים: טכנולוגיים, כלכליים, משפטיים, תקשורתיים ולעיתים גם פוליטיים ואף ביטחוניים.

אנו מבקשים לטעון ולהציע כי יש לזהות ולהגדיר את משברי הסייבר כסוג נפרד של משברים ארגוניים. שכן, אם אופיו ומהותו של משבר סייבר שונים מאלה של משברים אחרים, גם הטיפול התקשורתי והתדמיתי בו צריכים להיות שונים. בהתאם לכך יש לפתח אסטרטגיות וטקטיקות ייחודיות להתמודדות נכונה עם ההיבטים התקשורתיים והתדמיתיים של משבר הסייבר.

אתגר הטיפול בהיבט התקשורתי של משברי סייבר אינו רק נחלתם של אנשי יחסי הציבור של מי שנפגע או עלול להיפגע ממתקפת סייבר. הוא גם מציב אתגרים חדשים לפני העיתונאים הנאלצים להתמודד כיום עם עולם חדש, שרובו לא נודע ושונה.

## מהו משבר?

כל ארגון, גדול כקטן, עלול למצוא עצמו במצב של משבר. אך מהו, בעצם, משבר? אין הגדרה אחת, המקובלת על הכול, למונח זה (Coombs and Holladay, 2010). טימותי קומבס, המדגיש כי יש שפע של הגדרות למשבר, מציע הגדרה משלו: "סיכון משמעותי בעל פוטנציאל לתוצאות והשלכות שליליות ומזיקות אם לא יטופל כראוי" (Coombs, 2007a). הוא מזהה שלושה סוגי סיכונים במשבר, הקשורים זה לזה: איום על שלום הציבור, הפסד כספי ופגיעה במוניטין. משברים מסוימים עלולים לחולל אסונות ואובדן חיי אדם (Coombs, 2007b).

הגדרה ישנה, המבקשת לאפיין מצב של משבר בשונה מאירועים בעייתיים אחרים, קובעת שלמשבר יש שלושה מאפיינים: "הוא מאיים על ערכים בעלי חשיבות עליונה לארגון, מחייב תגובה בתוך זמן קצר ומתחולל במפתיע ובאופן בלתי צפוי" (Hermann, 1963, p. 64). חוקרים אחרים מדגישים כי משבר הוא אירוע או סדרת אירועים בלתי צפויים ובעלי רמות גבוהות של אי-ודאות וסיכון או פוטנציאל איום על יעדי החשובים ביותר של הארגון (Ulmer, Sellnow and Seeger, 2007). הגדרה מוכרת נוספת של משבר היא "אירוע בלתי צפוי המאיים על ציפיות חשובות של בעלי עניין, ועלול להשפיע באופן חמור על תפקודו של הארגון ולחולל תוצאות שליליות" (Coombs, 2007a, pp. 2-3). כמובן, עדיין שרירה וקיימת הקביעה שמשבר הוא מצב שעמו אין היחיד, הקבוצה או הארגון מסוגלים להתמודד בתהליכי עבודה שגרתיים, כתוצאה מלחצים שמקורם בשינוי פתאומי (Barton, 1993, מצוטט אצל Heath and Millar, 2008).

ארגון הבריאות הבינלאומי הציע הגדרה למשבר בריאות, לפיה משבר הוא "מצב לא יציב של סכנה או קושי קיצוניים". הארגון הדגיש כי בתחום הבריאות יש קשר קרוב בין בריאות ובין תקשורת, וכי כל המשברים בתחום הבריאות הם גם משברי תקשורת (World Health Organization, 2004). מזכ"ל ארגון הבריאות העולמי אמר על ההתמודדות עם משבר מגפת הקורונה, שהתפשטה ברחבי העולם בראשית העשור השלישי של המאה ה-21, כי נלחמים לא רק במגפה (pandemic) אלא גם במגפת-מידע (info-demic) (The Covid-19, 2020). דומה שהדברים הללו יפים גם למשברי סייבר.

יש המציעים להבחין בין שלושה סוגי משברים. האחד, משבר מידי שפורץ בדרך כלל ללא התרעה. אסונות טבע, כמו צונאמי או רעידות אדמה, הן דוגמאות לכך. הסוג השני הוא משברים המתפתחים באיטיות ואפשר להאט או לעצור אותם; מגפת הקורונה היא דוגמה לכך. הסוג השלישי הוא משבר מתמשך (prolonged crisis) העלול להימשך שבועות, חודשים או שנים (Parsons, 1996, מצוטט אצל Ritchie et al., 2003). בכל

אחד משלושת סוגי המשברים הללו ממלאים אמצעי תקשורת ההמונים תפקיד משמעותי (Avraham, 2009).

## משבר ותקשורת

המספר הגדול והולך של משברים בתחומים שונים של חיינו שיש להם היבטים תקשורתיים, הביא בעקבותיו גם עיסוק גובר בסוגיה זו, הן של אנשי אקדמיה הן של אנשי מקצוע, ואף להתמקצעות של אנשי יחסי ציבור העוסקים במצבי משבר בתקשורת. מה הפך את סוגיית התקשורת במצבי משבר, בתוך שנים לא רבות, לנושא כה חשוב? למגמה זו יש כמה הסברים חלופיים ומשלימים, הנעוצים בתמורות חברתיות, תקשורתיות וטכנולוגיות שהתרחשו בעיקר בשני העשורים האחרונים של המאה העשרים ובעשור הראשון של המאה העשרים ואחת (לימור, לשם ומנדלזיס, 2014).

לא רק הגדרת המושג "משבר" היא בעייתית; יש גם אי בהירות באשר למשמעות המדויקת של המושג "תקשורת במצבי משבר" או "משבר תקשורתי" (לימור, לשם ומנדלזיס, 2014). יש חוקרים הסבורים כי במושג זה מקופלות שתי מערכות נפרדות: האחת, איסוף והפצת מידע על המשבר, והשנייה – גיבוש האסטרטגיה שתינקט כדי להתמודד עם המשבר, תוצאותיו והשלכותיו (Coombs, 2004). קתלין פרן-בנקס אף מציעה להבחין בין שני מונחים, "משבר" ו"משבר תקשורתי". הראשון מתייחס למשבר בתוך הארגון אך אינו מגיע לידיעת אמצעי התקשורת ומהם לציבור, ואילו השני פירושו משבר שהדיו מגיעים לתקשורת ולציבור (Fearn-Banks, 2007, pp. 8-9).

משבר תקשורתי מתחיל כאשר אמצעי תקשורת ההמונים מודעים למשבר הפוקד את הארגון. מרגע זה על הארגון להתמודד לא רק עם המשבר עצמו, אלא גם עם היבטיו התקשורתיים והציבוריים. לא כל משבר בארגון מתפתח למשבר תקשורתי. הדברים נכונים גם לאירועי סייבר, אף אם הם מקבלים ממד של משבר ברמה הארגונית. בכך דומים משברי סייבר למשברים אחרים בתחומי הכלכלה, הבריאות או אסונות הטבע, שמקצתם מתפתחים למשברים תקשורתיים בעלי הד ציבורי ופרופיל תקשורתי גבוה, בעוד אחרים נעלמים ממסכי הרדאר הציבורי והתקשורתי. ראוי לזכור כי התפתחות משבר תקשורתי בכל תחום אינה קשורה בהכרח לגודל האירוע או להיקפו. במילים אחרות: אין קשר הכרחי בין עוצמת המשבר הממשי (כולל בתחום הסייבר) לזה התקשורתי.

יש הסבורים, כאמור, כי מה שהופך משבר בארגון, גם אם הוא קשור לתחום הסייבר, למשבר תקשורתי, הוא השלב שבו המשבר בארגון הופך לנחלת הציבור באמצעות תקשורת ההמונים (לימור ולשם, 2017), שמפרסמת ומהדהדת אותו. אנו מבקשים להציע כי במשבר סייבר, וכנגזרת ממנו גם במשבר תקשורתי, מעורבים תוקף ומותקף (תרשים 1). משבר שנגרם בגלל תקלה טכנית או טעות אנוש, אם כן, גם אם יש לו היבטי סייבר, לא יוגדר כמשבר סייבר.

העיסוק הגובר והולך במשברי תקשורת (או משברי תדמית) הביא גם לפיתוח דגמים ותיאוריות לטיפול בהם. שתיים מהתיאוריות הבולטות הן "תיאוריית מצבי משבר תקשורתיים" (SCCT – Situational Crisis Communication Theory) (Coombs, 2007c) וגישת "שיקום התדמית" (Image Restoration) (Benoit, 1995).

דומיניק הייל מבחין בין משבר תדמיתי (ולענייננו משבר תקשורת) ובין סוגים אחרים של משברים בארבעה עניינים (Heil, 2018). ראשית, התדמית של ארגון נוצרת ומעוצבת מחוץ לארגון עצמו ואינה בשליטתו; שנית, משבר תדמיתי מתחולל יחד עם סכנות נוספות המשפיעות על הארגון; שלישית, אי אפשר להשליך את המשבר על אחרים, וקשה לכמת אותו; רביעית, אם המשבר מנוהל בצורה נכונה, הוא עשוי ליצור הזדמנות לשיפור התדמית והשם הטוב של הארגון.

האומנם מתאימות התיאוריות הללו להגדרת משברי תקשורת ולדרך ניהולם גם בתחום הסייבר? אנו טוענים כי משברי סייבר – ומשברי תקשורת כחלק מהם – הם ייחודיים, ועל כן מחייבים פיתוח דרכי התמודדות וניהול שונים.

תחילה נבקש לזהות סוגים שונים של משברים ולאפיין את משבר הסייבר – וממילא גם את ההיבט התקשורתי שלו – כמשבר ייחודי. אנו מציעים לפיכך להבחין בין שישה סוגים שונים של משברים: משבר כלכלי, משבר ביטחוני-צבאי, משבר כתוצאה מפעולת טרור אסטרטגית, משבר בריאותי, אסון טבע וכן משבר סייבר. בלוח 1 מוצגים המשברים השונים ומאפייניהם, שמהם עולה כי משבר הסייבר הוא אכן משבר בעל מאפיינים ייחודיים לו.

### לוח 1: סוגים שונים של משברים ומאפייניהם

| סוג המשבר / מאפיינים  | סייבר                   | כלכלי   | ביטחוני / מלחמה <sup>4</sup> | טרור                   | בריאות   | אסון טבע |
|-----------------------|-------------------------|---|------------------------------|------------------------|----------|----------|
| מקור / יזם האירוע     | מאדם פרטי עד מדינה      | מגזר או תת-מגזר של המערכת הכלכלית ברמה לאומית או בין-לאומית | מדינה                        | קבוצת טרור או אדם פרטי | טבעי     | טבעי     |
| זהות המקור / היזם     | ברוך כלל אנונימי        | ברוך כלל מוזהה  | מוזהה                        | ברוך כלל מוזהה         | מוזהה    | ---      |
| מרחב ההכחשה מצד התוקף | רחב                     | מוגבל   | מוגבל                        | מוגבל                  | מוגבל    | ---      |
| מכוונות               | אירוע מכוון (מצד התוקף) | לא מכוון  | מכוון (ע"י התוקף)            | מכוון (ע"י התוקף)      | לא מכוון | לא מכוון |

| סוג המשבר / מאפיינים             | סייבר  | כלכלי   | ביטחוני / מלחמה <sup>4</sup>                         | טרור  | בריאות  | אסון טבע  |
|----------------------------------|--|---|--|---|---|---|
| תגובת נגד – מגיב ותגובה          | במקרים רבים צפויה מתקפת נגד מצד המדינה שבה בוצעה התקיפה, וכן הגנה על הארגון שהותקף | תגובה מוגבלת מצד המדינה נגד היום, אך בעיקר אמצעי ולסיוע להתגבר על המשבר | תגובה מצד המדינה שהותקפה וכן סיוע לנפגעים            | בדרך כלל מתקפת-נגד מצד המדינה וכן סיוע לנפגעים            | סיוע ברמה לאומית או אזורית, כולל אמצעי חיסון לאוכלוסייה                   | פעולה ממשלתית ברמה אזורית או לאומית, ובעיקר סיוע ושיקום |
| רמה וקצב התפתחות המשבר           | גמישה – ממהיר ומיידי עד איטי וארוך טווח  | בדרך כלל תהליך ארוך המתפתח באיטיות                                      | רחבים – ממידי עד ארוך טווח                           | בדרך כלל מיידי  | בדרך כלל איטי וממושך  | בדרך כלל מיידי  |
| מגזרים / תחומים המושפעים מהאירוע | רבי-מגזרי  | כלכלה   | המערכת הצבאית, אך גם את הכלכלה ותחומים אזרחיים אחרים | פגיעה בתחום האזרחי, אך בדרך כלל מוגבלת ברמה מקומית        | המצב הבריאותי של האוכלוסייה ברמה מקומית/ארצית וכן השפעה על המערכת הכלכלית | פגיעה בחיים אדם ופגיעה אפשרית במערכת הכלכלית            |
| סכנה לחיי אדם                    | בדרך כלל לא  | בדרך כלל לא   | בדרך כלל מוגבלת                                      | בדרך כלל מוגבלת   | עלולה להיות גבוהה מאוד  | עלולה לפגוע בחיי רבים                                   |
| יכולת להערכת הנזקים              | סוגיה מורכבת; התהליך עלול להיות ממושך  | יש אפשרות להערכת נזקים בכל אחד משלבי המשבר                              | הערכה מיידיה אפשרית                                  | הערכה מיידיה אפשרית                                       | הערכה מיידיה לא אפשרית; תיתכן הערכה בשלבים שונים של המשבר                 | בדרך כלל אפשרית באופן מיידי                             |
| שיקום                            | טווח זמן נרחב: ממהיר ומיידי ועד איטי וממושך  | תהליך ממושך   | בדרך כלל בטווח קצר                                   | בדרך כלל בטווח קצר  | ארוך טווח   | ארוך טווח   |
| אזהרה מוקדמת                     | בדרך כלל אין אזהרה מוקדמת  | בדרך כלל יש סימני אזהרה מוקדמים   | בדרך כלל יש סימני אזהרה מוקדמים                      | בדרך כלל אין אזהרה מוקדמת                                 | בדרך כלל אין אזהרה מוקדמת   | בדרך כלל אין אזהרה מוקדמת, אך לעיתים יש סימנים מוקדמים  |
| טווח הזמן של הנזק                | ממיידי עד ארוך טווח  | מטווח קצר עד ארוך   | ממיידי עד ארוך טווח                                  | בדרך כלל מיידי  | טווח בינוני עד ארוך   | ממיידי עד ארוך טווח                                     |
| היקף וחומרת המתקפה               | מנעד רחב – מקומית עם נזק כלכלי מועט ועד אירוע ברמה לאומית                          | מנעד רחב של נזק כלכלי   | מנעד רחב עם אפשרויות לקורבנות                        | בדרך כלל פגיעה ברמה מקומית עם אפשרות למספר קטן של קורבנות | מנעד רחב עם אפשרות למספר גדול של קורבנות                                  | מנעד רחב עם אפשרות לקורבנות                             |

| סוג המשבר / מאפיינים                                  | סייבר   | כלכלי                  | ביטחוני / מלחמה <sup>4</sup>        | טרור                   | בריאות  | אסון טבע                        |
|---|---|------------------------|-------------------------------------|------------------------|---|---------------------------------|
| יכולת הערכה מיידית של הנזק                            | נמוכה, כאשר הנזקים מתגלים, בדרך כלל, בשלבים ובאיטיות              | גבוהה                  | גבוהה                               | גבוהה                  | בינונית-נמוכה במיוחד כאשר הגורם למגפה לא מוכר | גבוהה                           |
| היעד של הביקורת הציבורית                              | בדרך כלל הגוף שהותקף  | הגורמים האחראים למשבר  | בדרך כלל, הגורם התוקף               | בדרך כלל, הגורם התוקף  | בדרך כלל מחולל האירוע                         | הרשויות – ברמה מקומית או לאומית |
| למי יאמין הציבור?                                     | לעיתים לגורם התוקף  | בדרך כלל לצד המותקף    | לצד המותקף                          | לצד המותקף             | לצד המותקף                                    | לצד המותקף                      |
| מודעות ציבורית לגורמי המשבר                           | לעיתים מוסתר דבר קיום האירוע מידיעת הציבור                        | האירוע גלוי וידוע לכול | האירוע גלוי וידוע לכול              | האירוע גלוי וידוע לכול | האירוע גלוי וידוע לכול                        | האירוע גלוי וידוע לכול          |
| היקף המדווח לציבור                                    | בדרך כלל מוגבל, כי שני הצדדים – המותקף והתוקף – ממעטים למסור מידע | רחב עד מלא             | רחב עד מלא                          | רחב עד מלא             | רחב עד מלא                                    | רחב עד מלא                      |
| היקף מידע כוב (פייק ניוז) ומידע מסולף (ריסאינפורמציה) | קרקע פורייה לחדשות כזב ולמידע מסולף                               | מוגבל                  | קרקע פורייה לחדשות כזב ולמידע מסולף | מוגבל                  | קרקע פורייה לחדשות כזב ולמידע מסולף           | מוגבל                           |
| תדירות אירועים מסוג זה                                | באופן קבוע  | נדירה                  | נדירה                               | נמוכה                  | נדירה   | נדירה                           |
| מגוון המטרות והנזקים                                  | נרחב מאוד   | מוגבל לסקטור הכלכלי    | נרחב                                | נרחב                   | מוגבל (בדרך כלל לאזור מסוים או רק לבני אדם)   | מוגבל (לאזור מסוים)             |
| היבט אידיאולוגי                                       | לעיתים  | נדיר                   | במקרים מסוימים                      | במרבית המקרים          | ---   | ---                             |

## המאפיינים הייחודיים של משבר סייבר

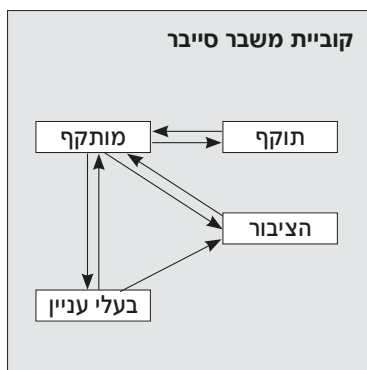
עיון בלוח 1 מלמד כי למשבר סייבר יש שורה של מאפיינים ייחודיים, המבדלים אותו מסוגים אחרים של משברים. בין אלה: ההיקף הפוטנציאלי הנרחב של הנזקים הנגרמים ממשבר סייבר, שהוא תוצאה של מתקפה; המנעד הרחב של רמת התפתחות המשבר וקצבו; או הקושי להעריך את הנזקים האמיתיים שנגרמו וייגרמו כתוצאה מהמשבר. יש המודגשים כי גילוי מתקפת סייבר עלול להיות איטי וממושך, במיוחד אם המותקף אינו מזהה את עצם קיומה, בגלל אופיה המיוחד (Ulsch, 2014; Sheppard et. al., 2013).

למשבר סייבר, בשונה ממשברים אחרים, עשויים להיות מחוללים שונים: מאדם פרטי, דרך קבוצה או ארגון וכלה במדינה. מאפיין אחר הוא שבמרבית המקרים זהות התוקף או מחולל המשבר נותרת אנונימית – בשונה ממשברים אחרים – והדבר מותיר ליזם האירוע מרחב הכחשה. למעשה, מרחב ההכחשה הוא כר נרחב לפעילות או לאי-פעילות, הן מצד התוקף הן מצד המותקף. במקרים רבים התוקף נמנע מלזהות עצמו, מכחיש את מעורבותו, מערפל את זהותו ויש קשיים אובייקטיביים בחשיפתו. במקרים מסוימים עשויים גורמים מודיעיניים לאתר אותו, אך הם נמנעים מלחלוק את המידע עם הציבור הרחב, לעיתים גם עם המותקף עצמו. במקרים רבים מוכחשת התקיפה על ידי הגוף המותקף, או שהמותקף נמנע ממסירת מידע לציבור, וכל אלה רק מגדילים את מרחב ההכחשה ומעצימים אותו.

מהו אפוא משבר סייבר והאם אפשר למצוא לו הגדרה ייחודית? התשובה אינה פשוטה. יש הגדרות שונות, ונציין שתיים מהן. מערך הסייבר הלאומי של ישראל קובע כי משבר בתחום הסייבר (Cyber Crisis) הוא "מצב שיש בו איום ממשי לפגיעה בנכס סייבר חיוני, או פגיעה בו בפועל, אשר עלול לגרום נזק קריטי לשגרת הפעילות ולתדמית, נזק כלכלי ופגיעה בחיי אדם"<sup>5</sup>. עוד נקבע כי "משבר סייבר נע במדרג רמות חומרה, ובמצב קיצון נגרם נזק ניכר לתהליכי ליבה ולרציפות התפקוד הארגוני/המשקית, והוא עלול להסלים עד כדי מצב חירום לאומי" (תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר, [ללא תאריך], עמ' 8). הסוכנות לאבטחת רשתות ומידע של האיחוד האירופי (ENISA – The European Union Agency for Cybersecurity) מגדירה משבר סייבר כאירוע יוצא דופן, שונה ממצב רגיל, שגלומה בו הפרעה רצינית או סכנה להפרעה כזאת, לתפקודים חברתיים חיוניים. משבר סייבר עלול לחצות גבולות לאומיים או גיאוגרפיים (ENISA, 2016).

מתקפת סייבר, שפירושה השגת שליטה ללא רשות במערכת מידע או שיבוש מכוון של מערכות כאלה, הופכת למשבר כאשר יש איום ממשי לפגיעה בנכס דיגיטלי חיוני או פגיעה בו בפועל. פגיעה כזאת עלולה לגרום נזק קריטי לשגרת הפעילות ו/או לתדמית, לנזק כלכלי ולפגיעה בחיי אדם. מבחינה זו יש אפוא דמיון רב בין נסיבות הרקע למשבר סייבר לאלה של משברים תקשורתיים במצבי מלחמה או טרור, שגם בהם יש תוקף ומותקף. על כן אפשר שכל היערכות עתידית לקראת משברי תקשורת בתחום הסייבר ראוי שתסתייע בידע ובניסיון שנצברו במשברים בנושאי ביטחון וטרור.

## תרשים 1



בתרשים 1 מוצגת "קוביית משבר הסייבר", שבמוקדה עומדים התוקף והמותקף (או המותקפים). ההשלכות של מתקפת הסייבר עשויות לחול על קבוצות מסוימות של בעלי עניין (למשל: לקוחות של חברה שמאגר המידע שלה הותקף ונפרץ), או על הציבור כולו (לדוגמה: פגיעה במערכת חשמל, אזורית או ארצית). במילים אחרות, אף שהמתקפה מכוונת נגד הגוף המותקף – ארגון ממשלתי, ציבורי או פרטי – הנפגעים המיידיים הם בדרך כלל בעלי העניין, כגון לקוחות של ארגון שהותקף, או הציבור הכללי, שבאים בטענות או בתביעות לגוף המותקף. טענות ותביעות כאלה נובעות מכך שגופים ממשלתיים וציבוריים, כמו גם ארגונים פרטיים רבים, מחזיקים ברשותם – אם מכוח החוק ואם משום שהמידע נמסר להם מרצון – במידע רב על אזרחים, כולל מידע אישי ופרטי. מכאן גם הציפייה שעל מחזיקי המידע לנקוט דרך קבע פעולות לאבטחת המידע, ומנגד להבטיח שקיפות ציבורית ולספק לציבור הסברים נכונים ומדויקים על הסיבות לכך שמאגרי המידע נפרצו וכתוצאה מכך התחולל משבר סייבר, שהביא גם למשבר תקשורתי ותדמיתי לארגון.

במקרים מסוימים עשוי הגוף המותקף, במיוחד אם המתקפה היא נגד גוף מדינתי, להגיב במתקפת נגד, בין שהדבר נעשה ביוזמת הגוף המותקף ובין שכמענה ללחצים ציבוריים.

### מדוע שונה משבר סייבר תקשורתי ממשברי תקשורת אחרים?

משבר סייבר, כמו כל משבר אחר בארגון, עלול להתחולל בדרגות חומרה שונות. במקרים רבים עלולה מתקפת הסייבר לגרום נזק ניכר לתהליכי ליבה ולרציפות התפקוד הארגוני. משבר כזה מלווה בדרך כלל בסיקור תקשורתי נרחב ומתמקד, בין השאר, בחולשות של מנגנוני ההגנה של הגוף המותקף או של הגורמים המופקדים על הגנת מרחב הסייבר במדינה.



אירוע סייבר משברי, שנגרם בו נזק משמעותי והשלכות רב-ממדיות ומעורר עניין רב בציבור, יכול לדרוך ככלל את המאפיינים הבאים (כולם או חלקם):

- סיקור תקשורתי נרחב. במקרים רבים ימלאו הרשתות החברתיות תפקיד מפתח כגורם הפצה של מידע, כולל מידע מסולף או כוזב, הן בכוונה הן שלא בכוונה.
- פניות רבות של עיתונאים לקבלת מידע ותגובות.
- מידע מסולף ומידע מוטעה (מיסאינפורמציה), שמקורם עלול להיות בעיקר התוקף, המפיץ אותם בכוונה. במקרים רבים עלול דווקא הגוף המותקף להפיץ מידע כוזב או מסולף, בעיקר כדי להסתיר את היקף הפגיעה במערכות הסייבר ואת ממדי הנזקים.
- הופעות רבות במדיה של מרואיינים ומומחים המייצגים לא אחת דעות שונות ומנוגדות.
- מתן הנחיות והמלצות לציבור או לגופים כדי להימנע מפגיעות אפשריות דומות.
- ביקורת רבה, בעיקר על הגוף המותקף.
- ביקורת על תפקוד המערכות השלטוניות האמורות להגן על כלל הארגונים במדינה. הציבור אינו מבחין תמיד בחלוקת האחריות ההגנתית בין המדינה לבין גופים פרטיים, דבר שגורם לטשטוש הגבולות והאבחנות בין ציבורי ופרטי.
- הביקורת עלולה להיות מלווה בתופעות של משבר אמון במערכות ההגנה, ברמת המדינה או הארגון, ובמקרים רבים גם בהתעוררות של דרישה לפעולה/תגובה של המדינה בעקבות האירוע. במקרים רבים ייטה הציבור לייחס אמון גבוה יותר לתוקף, מאשר למותקף.
- סייבר הוא שיח טכנולוגי מורכב שאינו מובן ברובו לציבור; כתוצאה מכך יש פערי ידע בין קבוצות שונות באוכלוסייה.

לאלה יש להוסיף גם את הקשיים בהערכת הנזקים והיקפם, במיוחד אם המתקפה אינה מהלך יחידני אלא שרשרת של פעולות, שבחלקן אינן גלויות והן בבחינת "זריעת מטעני חבלה" שיתפוצצו במועדים מאוחרים יותר. חקירה של תקיפת סייבר משולה מבחינות רבות להרכבת תצרך (פאזל), ולכן עשויה להימשך זמן רב. יש לכך סיבות מספר: לעיתים יש קושי להוכיח את זהות התוקפים; תמונת המצב הראשונית על היקף הנזק ומאפייני תקיפת הסייבר היא לעיתים קרובות מוגבלת וחלקית, במיוחד בשלבים הראשונים לאחר התקיפה.

סוגיית הנזקים והיקפם מחמירה משנה לשנה. הנזקים כוללים לא רק פגיעה ישירה בפעילות או בעסקים של הגוף המותקף,<sup>6</sup> אלא גם אובדן הכנסות עתידיות ומוניטין וכן קנסות מהרשויות הממלכתיות בגלל אי נקיטת אמצעי זהירות מספיקים למניעת מתקפת סייבר. כך, לדוגמה, נזקי המתקפה על אולפני "סוני" בשנת 2014 הוערכו בכמאה מיליון דולר (Richwine, 2014), ואילו חברת תעופה בריטית נקנסה בסכום של עשרים מיליון ליש"ט בגלל חשיפתה למתקפת סייבר (British, 2020). לפי הערכות שונות היקף הנזקים שייגרמו בשנת 2025 כתוצאה ממתקפות סייבר בכל רחבי העולם עשוי להגיע ליותר מעשרה טריליון דולר (Morgan, 2020).

- למשברי סייבר, ולמשברי סייבר תקשורתיים, יש כמה מאפיינים ייחודיים:
1. משברי סייבר מונעים על ידי טכנולוגיה, אך הם פוגעים או עלולים לפגוע גם בבני אדם ולהשפיע על חייהם.
  2. תקיפת סייבר היא מערכה שקטה, שאינה גלויה לעין. לא אחת מתגלה התקיפה לאחר זמן או רק לאחר שנחשפו הנזקים שנגרמו כתוצאה ממנה.
  3. העניין התקשורתי עשוי להיות גדול גם כאשר הנזק בפועל הוא קטן, כאשר מעורבים באירוע אישיות ציבורית, יעד בעל פרופיל תקשורתי גבוה או סמל שלטון. כך הם פני הדברים גם כאשר זהות התוקף היא בעלת חשיבות רבה יותר, למשל: מתקפה על ידי מדינה, לעומת מתקפה על ידי פצחן (האקר) בודד.
  4. הפרסומים על הצלחה של תקיפת סייבר עלולים לפגוע בתדמית הגוף המותקף, בעיקר ככזה שנתפס כבלתי אחראי או שנכשל בשמירה על המערכות שלו, ולעיתים גם על מערכות ההגנה ברמת המדינה, לערער את אמון הציבור במערכות ההגנה, ואף לעודד תקיפות נוספות.
  5. במקרים רבים מטרת התקיפה היא תודעתית, כלומר ליצור הד ציבורי באמצעות תקשורת ההמונים והרשתות החברתיות, לפעולת התקיפה ולהצלחתה, כדי לעורר הד נרחב לפעילותו של התוקף. פעילות התגובה התקשורתית חייבת להיות ערוכה להתמודדות במישור זה.
- מכל סוגי תקיפות הסייבר, תקיפת הכופרה (ransom) היא, ככל הנראה, השכיחה ביותר. אירוע של תקיפת כופרה הוא מורכב משום שהארגון המותקף מקיים משא ומתן עם התוקף. באירועים כאלה גם האסטרטגיה התקשורתית היא חלק מהמשא ומתן, כך שבניהולן נדרש תיאום מלא בין אנשי המשא ומתן לאנשי התקשורת, וכל מידע שבכוונת הארגון לפרסמו צריך להיבחן גם בעיני האחראים למשא ומתן. זאת ועוד, במקרים רבים גם התוקף מתנהל מול הארגון בפלטפורמות פומביות. זהו "חומר בערה" למשבר התדמית ועלול להשפיע על הימשכות המשבר התקשורתי.

### **שלבים בהתמודדות עם משבר בתקשורת סייבר**

לצורך המחקר הנוכחי אנו מציעים להבחין בין שני סוגים של משברי סייבר. האחד, משבר שנגרם בגלל תקלה טכנית או אנושית, ולמעשה אינו שונה במהותו ממשברים בארגונים אחרים, והשני – משבר שנגרם בגלל מתקפה מכוונת. המחקר הנוכחי מתמקד במשבר מהסוג השני, שיש בו תוקף ומותקף, כאשר המתקפה היא הגורם למשבר ארגוני ותקשורתי בגוף המותקף.

תקיפות ומשברי הסייבר הן אירוע צפוי ובה בעת בלתי צפוי לחלוטין. הן צפויות, כי מרבית המערכות כיום ממוחשבות ולכן הן פגיעות, ולו מבחינה פוטנציאלית, למתקפות מצד גורמים רבים ושונים שיש להם מוטיבציות מגוונות ובעיקר יכולות תקיפה המבוססות על טכנולוגיות מתקדמות. מצד שני, משבר סייבר ותקיפה אינם צפויים מבחינת עיתויים,

היקפם והנזק העלול להיגרם בגינם. במקרים רבים אין ארגונים נערכים כיאות לאפשרות של מתקפה משום שהם סבורים, בטעות, שהם קטנים מכדי לעורר עניין בתוקפים פוטנציאליים. ובפשטות: כיוון שמשבר ומתקפת סייבר הם כה צפויים יש להיערך, כמעשה של שגרה, למצב כזה. בפשטות: Expect the unexpected.

תרשים 2 משרטט הצעה לדגם של התמודדות ארגון מותקף עם משבר סייבר. יודגש: אין הכוונה למכלול ההיבטים הארגוניים והתפקודיים של המותקף כתוצאה מהמתקפה, אלא רק להיבטים התקשורתיים הכרוכים בטיפול במשבר. עם זאת, יש לזכור כי הטיפול התקשורתי במשבר איננו יכול להיעשות במנותק מהטיפול בהיבטים הארגוניים. השלב הראשון לאחר גילוי אירוע סייבר – לענייננו: מתקפת סייבר – הוא הערכת מצב ראשונית. במקביל להערכת הנזקים הממשיים שנגרמו באירוע ולאפיון הציבור שנפגע או שעלול להיפגע ממנו, יש לבצע הערכת נזק תדמיתי. במסגרת זו יש לנטר את הסיקור התקשורתי לאירוע, לבחון את היקפו ולהעריך את דפוסיו (לדוגמה: סיקור אוהד/ניטרלי/שלישי). כן יש לבחון את ההתנהגות התקשורתית של התוקף: האם הוא מזדהה או שומר על אנונימיות? האם הוא מעביר מידע לתקשור וכיצד?

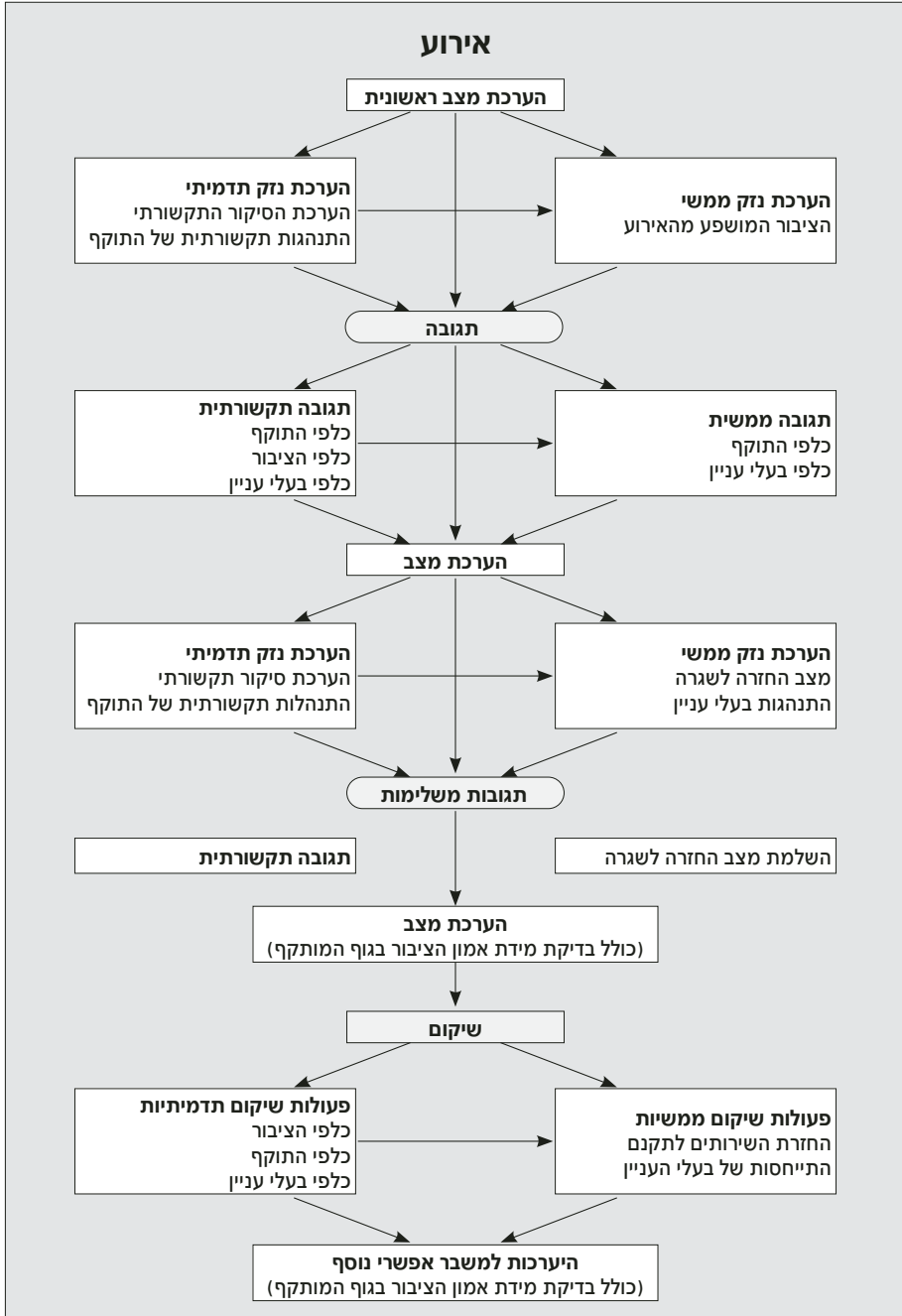
השלב השני הוא התגובה. יש להבחין בין תגובות מעשיות לתוקף, או תגובות המיועדות לבעלי עניין (למשל: לקוחות, ספקים, שותפים ואף הציבור הכללי), שאינן מעניינה של עבודה זו, ובין תגובות תקשורתיות. בהקשר זה יש לבחון ארבעה מוקדים לתגובות: כלפי התוקף, כלפי נפגעים ישירים, כלפי בעלי עניין אחרים וכלפי הציבור הרחב. התגובה התקשורתית חייבת להיות בהתאמה ובהלימה לתגובה המעשית, שכן פערים בין השתיים הם גורם לפגיעה באמון.

השלב השלישי הוא הערכת המצב. גם בשלב זה מתקיימות שתי פעילויות מקבילות ומשלימות. האחת מיועדת לבחון את הנזקים המעשיים שנגרמו כתוצאה ממתקפת הסייבר, את תיקונם ואת שלבי החזרה לשגרה, והשנייה – במישור התקשורתי. בשלב זה יש לבחון את היקף הסיקור התקשורתי ולהעריכו, ובמקביל גם לבחון את ההתנהלות התקשורתית של הגוף התוקף, כדי להגיב עליה ולהיערך להמשך פעילות נגדו.

השלב הרביעי הוא שלב התגובה המשלימה. ברמה הארגונית זהו השלב שבו חוזרת פעולת הארגון שנפגע, במלואה או בחלקה, לפעילות סדירה. במישור התקשורתי יש לבחון ולהחליט, כהמשך ישיר לשלב הקודם, אם יש צורך בתגובות תקשורתיות משלימות כלפי התוקף, כלפי בעלי העניין וכלפי הציבור הרחב.

השלב החמישי הוא שלב הערכת המצב. בשלב זה יש לבחון את ההצלחה של הארגון שנפגע לחזור לפעילות סדירה, בצורה מלאה או חלקית, וברמה התקשורתית לבחון את הצלחת התגובות התקשורתיות. בה בעת יש לבדוק, באמצעות סקרים ובכלים אחרים, אם חלה שחיקה ברמת האמון של הציבור הרחב ושל בעלי העניין בארגון שהותקף ובפעולותיו.

## תרשים 2: משבר סייבר: ההיבט התקשורתי



השלב השישי הוא שלב השיקום. זה השלב שבו הארגון שהותקף מחזיר את פעילותו לרמה הרגילה וכל שירותיו מוחזרים לתקנם, ובמקביל גם משקם את יחסיו עם הנפגעים הישירים ועם בעלי העניין השונים. במישור התדמיתי נערכות פעולות שונות שתכליתן לשקם את תדמית הארגון, כאשר מאמצי השיקום התדמיתי הם דיפרנציאליים ומשלימים ומנותבים כלפי הציבור הרחב, כלפי התוקף וכלפי בעלי העניין (כולל נפגעים ישירים). השלב השביעי הוא שלב החזרה לשגרה. אף על פי שלכאורה החיים חוזרים למסלולם הרגיל והארגון שהותקף יכול לתייק את האירוע בספרי ההיסטוריה שלו – לא כך צריכים הדברים להתנהל. ברמה הארגונית יש לבדוק ביסודיות כיצד התאפשרה התקיפה, ובעיקר להיערך לקראת משבר עתידי אפשרי, אם כתוצאה מכשל ארגוני או בגלל טעות אנוש, ואם כתוצאה ממתקפת סייבר. במישור התקשורתי יש להיערך, כולל הכשרת כוח אדם ייעודי ובניית כלי ההסברה הנאותים, לקראת המשבר הבא.

### **פרמטרים לאבחון משברי סייבר תקשורתיים ולניהולם**

מתקפת סייבר עלולה לגרום לנזקים שונים, ובראשם: חבלה בפעילות הארגון המותקף באמצעות מערכות ממוחשבות; נזקים כלכליים ופיזיים ברמה לאומית; נזקים כלכליים ופיזיים לארגון המותקף; גניבת כספים; גניבת נכסים אינטלקטואליים בתחום העסקי; גניבת מידע פנימי בתחומים העסקי, השלטוני או הביטחוני; גניבת מידע (כולל מידע מסווג ופרטי כרטיסי אשראי) לצורך התחזות או פשיעה. ביטוי לכך אפשר למצוא, לדוגמה, בדבריו של מנכ"ל בנק לאומי, חנן פרידמן, שטען כי "בנק שיעמוד בפני מתקפת סייבר ולא יוכל לספק שירותים במשך 24 שעות – כנראה יקרוס, כי הלקוחות ימשכו את הכסף ולא יאמינו שיוכל להשתקם".<sup>7</sup>

שלב ראשון באבחון משבר סייבר, ומשבר סייבר תקשורתי כחלק ממנו, הוא זיהוי המרכיבים השונים שעשויה להיות להם השפעה על עוצמת המשבר התקשורתי והיקפו. זיהוי מוקדם הוא כלי חשוב ויעיל לניהול המשבר התקשורתי וניהולו.

אפשר להצביע על שישה מרכיבים כאלה:

1. רמת התוקף: האם התקיפה נעשתה על ידי אדם בודד, על ידי קבוצה מאורגנת או על ידי מדינה.
2. חשיבות המותקף: האם המותקף הוא ארגון שלפעילותו יש השפעה על ציבור רחב, האם יעד התקיפה הוא גוף המעורב בפעילות העומדת על סדר היום הציבורי, או שמדובר בתקיפה בעלת ערך סמלי.
3. כיצד בוצעה התקיפה? האם התוקף ניצל פרצות במערכות ההגנה? האם היו מחדלים במנגנוני האבטחה?
4. מטרת התקיפה: תקיפה למטרות ריגול או טרור תזכה לחשיפה תקשורתית ותעורר הדים ציבוריים רחבים יותר מאשר תקיפה שנועדה למטרות גניבה או סחיטה.

5. ההצלחה של התקיפה: ההצלחה עשויה להימדד על פני קריטריונים שונים, אך במקרים רבים אין מדובר בהכרח בהצלחה ממשית אלא בדימוי ההצלחה או בתפיסת ההצלחה (אם מצד התוקף ואם מצד המותקף).

6. תגובת הנגד, אופיה והצלחתה: בהקשר זה ייבחנו היבטים כגון: מי המגיב, מה הייתה מטרת התגובה ואופיה, מה הייתה הצלחת התגובה, ובעיקר – האם התגובה פורסמה, ישירות או בעקיפין, על ידי הגורם המגיב.

כל השלבים הללו, והשאלות העולות במהלכן, הם בעלי חשיבות לא רק לארגון המותקף ולאנשי ההסברה ויחסי הציבור שלו, קרי למדיניות התקשורתית שתינקט על ידו כתוצאה מהמשבר, אלא גם לעיתונאים ולאנשי תקשורת המסקרים את המשבר.

### ניהול המשבר כאירוע תקשורתי

בעת גיבוש התוכנית האסטרטגית של ניהול משבר תקשורת בתחום הסייבר ראוי לזהות שישה קהלי יעד, שלגבי כל אחד מהם יש לנקוט פעולות נפרדות וייעודיות, אף שאלה חייבות להיות בהלימה ובהתאמה כמכלול אחד. שישה קהלי היעד הם: (א) ציבורים וגורמים המושפעים ישירות מהאירוע: לקוחות, ארגונים, אזרחים תושבי אזור מסוים וכולי; (ב) הציבור הכללי; (ג) עובדי הארגון; (ד) גורמי ממשל רלוונטיים; (ה) הזירה האזורית (במקרה של ישראל: הזירה המזרח-תיכונית); (ו) הזירה הבינ-לאומית (ראו לוח 2).

### לוח 2: אסטרטגיית הסברה: מטרת וקהלי יעד

| קהלי יעד  | מטרות ויעדים   |
|---|--|
| ציבורים וגורמים המושפעים ישירות מהאירוע: לקוחות, ארגונים, אחרים תושבי אזור מסוים וכו' | <ul style="list-style-type: none"> <li>• אספקת מידע אמין ותמונת מצב מדויקת</li> <li>• הנחיות והמלצות לפעולה לציבור ולארגונים שונים</li> <li>• הרגעה וחיזוק האמון בארגון המותקף ובמערכות הקשורות אליו, וביכולתן לטפל באירוע בהצלחה</li> <li>• הזמת שמועות ודיסאינפורמציה / ומידע מסולף</li> <li>• מענה לטענות נגד הארגון</li> <li>• תיאום מסרים עם כל הגורמים המעורבים</li> <li>• התאמת המסרים לתת הקבוצות השונות מבחינת רמת מודעות, יכולת טכנולוגית, השפה, הבדלי תרבות, אמצעי התקשורת הנחשפים ביותר וכן ניתוב מסרים באמצעות משפיענים וידוענים</li> </ul> |
| הציבור הכללי  | <ul style="list-style-type: none"> <li>• חיזוק האמון הציבורי בגוף המותקף ובמערכות ההגנה הרלוונטיות (רגולטורים, מערך הסייבר הלאומי)</li> <li>• הפגנת שקיפות</li> <li>• מענה לטענות כנגד הארגון</li> <li>• הזמת שמועות ודיסאינפורמציה / ומידע מסולף</li> <li>• תיאום מסרים עם כל הגורמים המעורבים</li> </ul>   |

| מטרות ויעדים   | קהלי יעד  |
|--|---|
| <ul style="list-style-type: none"> <li>• חיזוק האמון ביכולת ההנהלה לטפל במשבר.</li> <li>• רתימת העובדים להעברת מסרי הארגון</li> <li>• הפגנת שקיפות</li> <li>• הזמת שמועות ומידע מסולף</li> <li>• הקפדה על הימנעות של עובדי הארגון מביקורת חיצונית</li> </ul> | <p><b>עובדי הארגון</b><br/>(תקשורת פנים ארגונית)</p>                                |
| <ul style="list-style-type: none"> <li>• חיזוק האמון ביכולת הארגון להתמודד עם המשבר</li> <li>• הפגנת שקיפות</li> <li>• הזמת שמועות ומידע מסולף</li> <li>• גיוס גורמי ממשל להשגת יעדים בזירה האזורית והבינלאומית</li> </ul>                                   | <p><b>גורמי ממשל רלוונטיים:</b><br/>רגולטורים, מערך הסייבר, פקידים ונבחרי ציבור</p> |
| <ul style="list-style-type: none"> <li>• הרתעה</li> <li>• מניעת תודעת הישג מצד הגורם התוקף</li> </ul>  | <p><b>הזירה האזורית:</b><br/>יריבים ואויבים (ככל שהם רלוונטיים לאירוע)</p>          |
| <ul style="list-style-type: none"> <li>• חיזוק תדמית המדינה כמעצמת סייבר</li> <li>• הרתעה מהמשך תקיפות</li> <li>• מניעת תודעת הישג</li> <li>• גיבוש שותפים/קואליציה נגד התוקף</li> </ul>   | <p><b>הזירה הבינ-לאומית</b><br/>(ככל שהדברים רלוונטיים לאירוע)</p>                  |

## הדילמה ההסברתית: האם לדווח לתקשורת על האירוע?

אחת הסוגיות הראשונות שעמה מתמודדים בעת שמתרחשת מתקפת סייבר, או כאשר מתגלה ניסיון למתקפה כזאת על יעד בעל חשיבות ציבורית, היא אם לדווח על האירוע בצורה יזומה לאמצעי התקשורת ובאמצעותם לציבור הרחב.

התשובה על שאלה זו איננה חד-משמעית והיא תלויה בנסיבות האירוע ובאופיו. עם זאת אפשר להצביע על "כלל אצבע": קנה המידה העיקרי בעת גיבוש ההחלטה בנושא זה צריך להיות המבחן הציבורי, לאמור: האם יש לאירוע או עלולה להיות השפעה על הציבור, וכן מה יהיו היקפיה ומשמעויותיה, כולל המשמעויות של חשיפת התקיפה.

לשקיפות של הארגון המותקף כלפי הציבור עשויה להיות השפעה רבה על דעת הקהל ועיצובה, אך בה במידה היא עשויה להשפיע, על פי הניסיון שהצטבר בעולם, על המוטיבציה של התוקף להמשיך בפעילותו, כלומר המשך התקיפה. בעת קבלת ההחלטה אם לזום פרסום על האירוע – תקיפה בפועל או ניסיון תקיפה – יש להתחשב גם בהיבטים חוקיים, למשל: חובת דיווח לרגולטור רשמי, לחברת ביטוח, לכורסה, לרשות להגנת הפרטיות ועוד, והסדרים אחרים בין הארגון ובין ארגונים אחרים או לקוחותיו. כיצד פועלים אם נתקבלה החלטה לא לדווח על האירוע? במקרה כזה יש להכין "תגובה נצורה", וכן לקבוע ולהכשיר גורם מתאים לתדרוך המדיה, אם וכאשר יגיע שלב הפרסום, שיהיה בדרך כלל ביוזמת אמצעי התקשורת. כחלק מההיערכות יש להכין

גם מענה ברור ואמין על השאלה שיציגו העיתונאים והציבור: מדוע הוסתר המידע על האירוע ומדוע לא נמסרה עליו הודעה יזומה לציבור.

אם יוחלט למסור מידע לציבור, יש לשקול בזהירות מי יהיה הגורם או הדובר שיפרסם את המידע. האם יהיה זה הגוף שהותקף (ואם כן, מי ידבר מטעמו ובשמו)? האם יהיה זה הרגולטור האחראי על התחום או הארגון שהותקף? האם יהיה זה נציג מערך הסייבר הלאומי? ואולי המידע יימסר הודעה משותפת לכמה גורמים?

יש לזכור כי באירוע סייבר מעורבים בדרך כלל כמה גופים שאין בהכרח חפיפה והלימה בין האינטרסים שלהם. כך, כדוגמה, חברה עסקית תפעל בראש ובראשונה לצמצם את הנזק הכלכלי שנגרם או שעלול להיגרם לה ולשמור על תדמיתה, ולפיכך תשאף להמעיט ככל שתוכל בתיאור הנזק ובמחדלי הגנת הסייבר שלה ואף תנסה להטיל אחריות על גורם אחר (למשל על מדינה זרה או על היעדר הגנה מצד המדינה שבה פועלת החברה העסקית). לעומת זאת, גופים מדינתיים אמורים לראות בראש ובראשונה את האינטרס הציבורי הרחב ולעיתים אף ישאפו להציג את מחדלי הגורם המותקף כדי להעלות את המודעות הציבורית והמשקית לצורך בחיזוק הגנות הסייבר בכל הגופים.

### **מדוע ומתי מומלץ ליזום סיקור תקשורתי במקרה של מתקפת סייבר?**

אפשר להצביע על שורה של מצבים שבהם יש חשיבות למסירה יזומה של מידע לציבור במקרה של מתקפת סייבר. מנגד יש לא אחת סיבות ראויות להסתיר את המידע ולהימנע מהפצתו ברבים. אלה הנימוקים לפרסום יזום של מידע:

1. כאשר אי אפשר להסתיר את הפגיעה בציבור ואת הנזקים שנגרמו בתקיפה.
2. כאשר יש, או עלולה להיות, פגיעה בנכס אישי של אזרחים רבים, ועל כן יש להזהיר את הציבור מפני הסכנה. מצב זה דומה להתפרצות מגפה שיש להזהיר את הציבור מפניה ומפני החשש להתפשטותה.
3. כאשר נגרמה פגיעה או אירע ניסיון של פגיעה בשירות חיוני לציבור כגון תחבורה, אספקת מזון, שירותי בריאות, מים, חשמל וכולי.
4. כאשר נגרמה פגיעה בשירות שיש בו עניין לציבור (כמו המדיה, בתי קולנוע ועוד).
5. כאשר נגרמה פגיעה בארגון מסוים והדבר עלול לסכן ארגונים אחרים, שהמותקף קשור ומחובר אליהם.
6. כאשר נעשה ניסיון תקיפה בהיקף רחב על המשק שנכלם, הוכל או לא גרם לנזקים.
7. כאשר נגרמו, או עלולים להיגרם, שיבושים בתפקודם של מאגרי חשוכים מבחינה ציבורית.
8. כאשר האירוע היה תוצאה של פעילות אויב או של תקיפה מצד מדינה, והדבר עלול לזכות בהד תקשורתי נרחב (בדרך כלל, ביוזמת הגורם התוקף).
9. כאשר נגרמה פגיעה בנכס או בסמל ציבורי/ממשלתי בעלי חשיבות.



10. כאשר האירוע גרם פגיעה משמעותית במוסד פיננסי חשוב, והפגיעה עלולה לערער את האמון הציבורי במערכת הכלכלית כולה.
  11. כאשר הפגיעה נעשתה במקביל במספר ארגונים.
  12. כאשר האירוע מהווה "אירוע תודעתי", ו/או עלול להוות מוקד למידע מסולף.
  13. כאשר הפגיעה תהיה באתרי אינטרנט שיש להם חשיפה ציבורית נרחבת.
  14. כאשר הפגיעה תהיה בתשתית חיונית והיא עלולה לשבש את השירות לציבור.
  15. כאשר המתקפה נועדה או עלולה לפגוע בבריאות הציבור.
  16. כאשר יש דליפת מידע או חשש מדליפה כזאת.
  17. כאשר יש חשש לפרסום יזום על ידי התוקף, ולכן יש חשיבות להקדימו.
  18. כאשר החשיפה היוזמה עשויה להשפיע על התנהגות התוקף ולמנוע נזקים נוספים.
- הסיבות שתוארו לעיל מתייחסות למקרה שבו אין לגוף המותקף חובת דיווח לציבור. במקרים רבים יש לגוף המותקף חובת דיווח לציבור, ועל כן אין הוא יכול להימנע ממסירת מידע ומדיווח על האירוע. לדוגמה: חברות שיש להן ביטוח סייבר מחויבות לדווח לגורם המבטח שלהן על אירוע סייבר. חברות שנסחרות בבורסה בישראל או בעולם מחויבות לדווח על פגיעה כזו. יש גם אירועים שהגוף המותקף מחויב לדווח עליהם לרשות להגנת הפרטיות.
- מול השיקולים והגורמים לפרסום יזום של מידע במקרה של מקפת סייבר או ניסיון למתקפה כזאת, יש שורה של שיקולים נגד פרסום כזה. וביניהם:
1. חשש מיצירת בהלה או דאגה בציבור הרחב.
  2. מתן "פרס תודעתי" לגורם התוקף.
  3. מניעת מידע מהתוקף.
  4. התקיפה לא גרמה לנזק משמעותי או ציבורי, ועל כן אין חשיבות ועניין בפרסומה.
  5. התקיפה לא גרמה לפגיעה או לשיבוש בפעולה של גוף או שירות ציבורי.
  6. לאירוע אין השלכות המצדיקות פרסום הנחיות או המלצות לציבור.
  7. הגורם שהותקף, או המדינה שהוא חלק ממנה, מתכננים תגובה שקטה, והפרסום עלול לשבש את פעולת הנגד.
  8. האירוע הוכל ונמנע נזק ממשי.

### **"תודעת תוקף" במשבר סייבר**

המונח "תודעת תוקף", שבו אנו משתמשים עתה, שאוב בהשאלה ממילון המונחים הצבאי, ועוסק בהיבטים פסיכולוגיים ותודעתיים של האויב. לענייננו, המטרה המרכזית בתחום זה – כחלק מהפעילות התקשורתית-הסברתית בעת משבר סייבר – היא ליצור בתוקף תחושה של אי הצלחת התקיפה, של חסינות המותקף ושל האפקטיביות של מערכות ההגנה, כמו גם איום בדבר הנכונות להגיב בעוצמה נגד התוקף.

היעד המרכזי ברוב האירועים הוא להמעיט בהישגי התוקף, ועל כן יש לשוב ולהרהר את המסר הזה. עם זאת יש לנקוט זהירות בניסוח התגובה, בעיקר משום שלא תמיד, כאמור, הנזקים גלויים וידועים במלוא היקפם מייד עם גילוי האירוע. הפחתה או המעטה בעוצמת האירוע עלולים לגרום לכך שהתוקף יבצע מתקפה נוספת או שהוא יחשוף ברבים מידע שאליו הצליח לחדור – והדבר יפגע באמינות הגורם המותקף.

## סיכום

אירוע סייבר מציף בדרך כלל סדרה של סוגיות ושאלות שכל ארגון שהותקף חייב להיות ערוך להתמודד עימן כדי להשיב עליהן בצורה נאותה. בין אלה: כיצד התרחשה התקיפה ומדוע מנגנוני ההגנה לא הצליחו לבלום אותה? האם מטרת התקיפה לקבל כופר ומהי מדיניות הארגון בסוגיה זו? האם האירוע גורם להשבתה בשירות שהארגון מספק או משבש אותו? ואם כן, כמה זמן יידרש לתיקון המערכת ולהחזרתה לפעילות סדירה? האם המתקפה גרמה לשיבושים במידע, למחיקת מידע או לדליפת מידע?

אולם משבר סייבר – וכל שכן משבר תקשורתי בתחום הסייבר – אינו רק אתגר לארגון המותקף ולאנשי יחסי הציבור שלו. הוא מציב גם שורה של אתגרים וקשיים לעיתונאים ולאנשי התקשורת האמורים לסקר את האירוע ולדווח עליו. זאת במיוחד לאור המסתורין האופף את מתקפות הסייבר, לאור אי הוודאות סביב האירועים, נסיבותיהם ותוצאותיהם ולאור העובדה שמתקפות סייבר ומשברי סייבר הם כר פורה למידע כוזב, מידע מסולף ומידע מוטעה.

האתגרים והקשיים הללו הם בשלוש רמות: הראשונה, הידיעה על עצם קיומו של האירוע, במיוחד כאשר הציבור הרחב אינו חש, לפחות בשלב הראשון, במתקפה או בתוצאותיה; השנייה, קבלת מידע עדכני ואמין, במיוחד כאשר הגוף המותקף מסרב למסור מידע (וכל שכן כאשר התוקף מעדיף, משיקוליו שלו, לא לפרסם את דבר התקיפה ו/או את זהותו); השלישית, להבין את משמעות התקיפה והשלכותיה. בעוד בשתי הרמות הראשונות הפעילות העיתונאית דומה במידה רבה לזו המתנהלת בתחומים שונים של החיים, כאשר העיתונאים מנסים לפצח "קירות מגן" של ארגונים המסתירים מידע, או מסרבים לשתף פעולה עם התקשורת והציבור, עיסוק בתחום הסייבר מחייב היכרות עם העולם הטכנולוגי החדש והבנת דרכי פעולתו. בעוד במערכות אמצעי התקשורת יש עיתונאים שהתמחו בתחומי סיקור שונים, החל בכלכלה או צבא וכלה בנדל"ן ספורט, מעטים הם העיתונאים שיודעים להתמודד עם סוגיית סיקור משברי סייבר.

עולם הסייבר יוצר אפוא מציאות חדשה, הן לאנשי יחסי הציבור הן לעיתונאים, שתחייב כבר בעתיד הקרוב הכשרה הנאותה ורכישת כלים מתאימים להתמודדות נכונה ונאותה עם אתגריו.

## הערות

- \* המאמר מבוסס על עבודת מחקר שנערכה במסגרת המרכז הרב-חזומי לחקר הסייבר ע"ש בלווטניק באוניברסיטת תל אביב ובסיועו. המחברים מבקשים להודות לאנדריאה פולישוק שהייתה עוזרת המחקר בפריקט זה.
- 1 הנתונים מבוססים על מידע שנוטר על ידי חברת אבטחת המידע הישראלית צ'ק פוינט.  
ראו את דיווחי חברת אבטחת המידע הרוסית קספרסקי: <https://cybermap.kaspersky.com/stats>
  - 2 הדברים נאמרו בשנת 2018 בהרצאה בכנס בנושא סייבר. ראו: <https://quotepark.com/quotes/1778580-robert-mueller-i-am-convinced-that-there-are-only-two-types-of-co>
  - 3 מלחמה בעידן המודרני כוללת גם מתקפות סייבר, אך במקרה כזה נציע לכלול את מתקפת הסייבר כחלק מהפעילות המלחמתית הכוללת. על שימוש במתקפת סייבר כחלק מהארסנל הצבאי במלחמה ראו המקרה של תקיפת אוקראינה על ידי הצבא הרוסי בחודש פברואר 2022. לדוגמה: מימון, 2022.
  - 4 בדף הבית של מטה הסייבר הלאומי מוגדרות מטרותיו כדלקמן: "המעריך הוא גוף ממלכתי, ביטחוני וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל קידום וביסוס עוצמתה של ישראל בתחום. המעריך פועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הארגונים והאזרחים, לטיפול בתקיפות סייבר ולסילוקן ולהיערכות לחירום. כחלק מתפקידיו, מקדם המעריך פתרונות חדשניים וטכנולוגיות צופות פני עתיד, מתווה אסטרטגיה ומדיניות בזירות הלאומית והבין-לאומית, ומפתח את ההון האנושי בתחום". ראו: [https://www.gov.il/he/departments/israel\\_national\\_cyber\\_directorate/govil-landing-page](https://www.gov.il/he/departments/israel_national_cyber_directorate/govil-landing-page) (אוחזר בספטמבר 2022).
  - 5 דוגמה לכך היא המתקפה על חברת הנפט קולוניאל פיפללין שהשבייתה את צינור הנפט הגדול ביותר בארה"ב. ראו: Turton, W. and K. Mehrotra (4.6.2021), "Hackers Breached Colonial Pipeline Using Compromised Password". *Bloomberg*. Retrieved on 9.5.2022 from: <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>
  - 6 ראו שיחה עם חנן פרידמן (מאי 2021), במת ניהול חברה, אוניברסיטת תל-אביב. אוחזר ב-1.5.2022 מן האתר [https://www.youtube.com/watch?v=B\\_EO54samCc](https://www.youtube.com/watch?v=B_EO54samCc)

## מקורות

- לימור, י' וב' לשם ול' מנדלזיס (2017). איך להפוך צפרדע לנסיך: אלף טיפים ביחסי ציבור. ראשון לציון: ידיעות אחרונות.
- לימור, י', וב' לשם ול' מנדלזיס (2014). יחסי ציבור: אסטרטגיה וטקטיקה. רעננה: האוניברסיטה הפתוחה. מימון, ט' (2022). "המלחמה בין רוסיה לאוקראינה מוכיחה: חזית הסייבר היא שובר השוויון החדש", *גלובס*. נדלה ב-31.3.2022 מ: <https://www.globes.co.il/news/article.aspx?did=1001403486>
- תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר (ללא תאריך). ירושלים: משרד ראש הממשלה, מערך הסייבר הלאומי. נדלה ב-1.5.2022 מ: <https://www.gov.il/BlobFolder/news/cybercrisispreparedness/he/Management%20of%20crisis%20situations%20final.pdf>
- Avraham, E. (2009). "Marketing and Managing Nation Branding during Prolonged Crisis: The Case of Israel", *Place Branding and Public Diplomacy*, 5(3), pp. 202–212.
- Benoit, W.L. (1995). *Accounts, Excuses, and Apologies: A Theory of Image Restoration Strategies*. New York: State University of New York Press.
- British Airways fined £20m over data breach (2020). *BBC News*. Retrieved 8.5.2022 from BBC News site (16.10.2020): <https://www.bbc.com/news/technology-54568784>.

- Coombs, T. (2004). "Crisis Communication", *Encyclopedia of Public Relations*, SAGE Publications. Retrieved on 22.9.2009 from: <[http://www.sage-ereference.com/publicrelations/Article\\_n104.html](http://www.sage-ereference.com/publicrelations/Article_n104.html)>.
- Coombs, T. (2007a). "Crisis Management and Communications", Posted on the website of the *Institute of Public Relation (IPR)*. Retrieved on 28.9.2022 from: <https://instituteforpr.org/crisis-management-and-communications/>
- Coombs, T. (2007b). *Ongoing Crisis Communication: Planning, Managing, and Responding* (2nd ed.). Los Angeles: Sage.
- Coombs, W.T. (2007c). "Protecting Organization Reputations during a Crisis: The Development and Application of Situational Crisis Communication Theory", *Corporate Reputation Review*, 10(3), pp. 163-176.
- Coombs, T. and S. Holladay (eds.) (2010), *The Handbook of Crisis Communication*. Chichester, UK: Wiley-Blackwell.
- The Covid-19 Infodemic (2020). *The Lancet*. DOI: [https://www.thelancet.com/journals/laninf/article/PIIS1473-3099\(20\)30565-X/fulltext](https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30565-X/fulltext).
- ENISA – European Union Agency for Network and Information Security (2016). *Strategies for Incident Response and Cyber Crisis Cooperation*. Retrieved on 1.3.2022 from: <https://www.bitlylinks.com/QntPdRtx5>.
- Fearn-Banks, K. (2009). "Crisis Communication", in: W. Eadie (ed.), *21st Century Communication: A Reference Handbook* (pp. 741-748). Thousand Oaks, CA: Sage.
- Heath, R. & D. Millar (2008). *Responding to Crisis: A Rhetorical Approach to Crisis Communication*. Mahwah, NJ: Lawrence Erlbaum.
- Heil, D. (2018). "Reputation Risk", in: R. Heath, a& W. Johansen (eds.), *The International Encyclopedia of Strategic Communication* (pp. 1-6). Hoboken, NJ: Wiley-Blackwell.
- Herman, C.F. (1963). "Some Consequences of Crisis which Limits? the Viability of Organizations", *Administrative Science Quarterly*, 8, pp. 61-82.
- Morgan, S. (2020). "Cybercrime To Cost the World \$10.5 Trillion Annually by 2025". *Cybercrime Magazine*, 13.11.2020. Retrieved on 9.5.2022 from: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016>.
- Ritchie, B., H. Dorrell, D. Miller and G.H. Miller (2003). "Crisis Communication and Recovery for the Tourism Industry: Lessons from the 2001 Foot and Mouth Disease Outbreak in the UK", *Journal of Travel and Tourism Marketing*, 15, pp. 199-216.
- Richwine, L. (2014), "Cyber Attack Could Cost Sony Studio as much as \$100 million", *Reuters*, 10.12.2014. Retrieved on 28.9.2022 from: <https://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209>
- Sheppard, B., M. Crannell and J. Moulton (2013). "Cyber First Aid Proactive Risk Management and Decision-making", *Environment Systems and Decisions*, 33(4), pp. 530-535.
- Ulmer, R., T. Sellnow and M. Seeger (2007). *Effective Crisis Communication: Moving from Crisis to Opportunity*. Thousand Oaks, CA: Sage.
- Ulsch, N.M. (2014). "What Is the True Cost of a Cyber-attack?", in: *Cyber Threat!* (pp. 69–84). <https://doi.org/10.1002/9781118915028.ch04>
- World Health Organization (WHO) (2004). *Sixth Futures Forum on Crisis Communication*. Retrieved on 1.4.2022 from: [https://www.euro.who.int/\\_data/assets/pdf\\_file/0004/90535/E85056.pdf](https://www.euro.who.int/_data/assets/pdf_file/0004/90535/E85056.pdf).