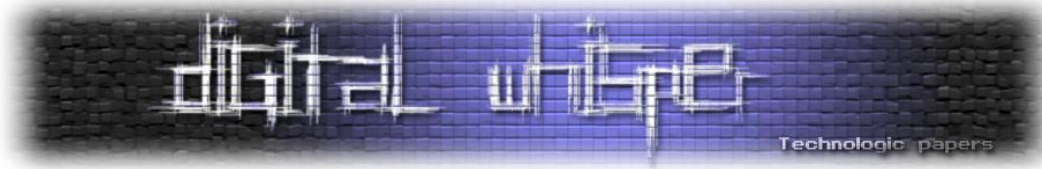


## המדריך לתייר בסמטאות האפלות של הרשת

**רקע**



## החלוקה של האינטרנט

למען הפשטות, אחלק את האינטרנט על-בסיס של נגישות למשתמש:

1. Surface Web.

2. Deep Web/Undernet.

3. Dark Internet.

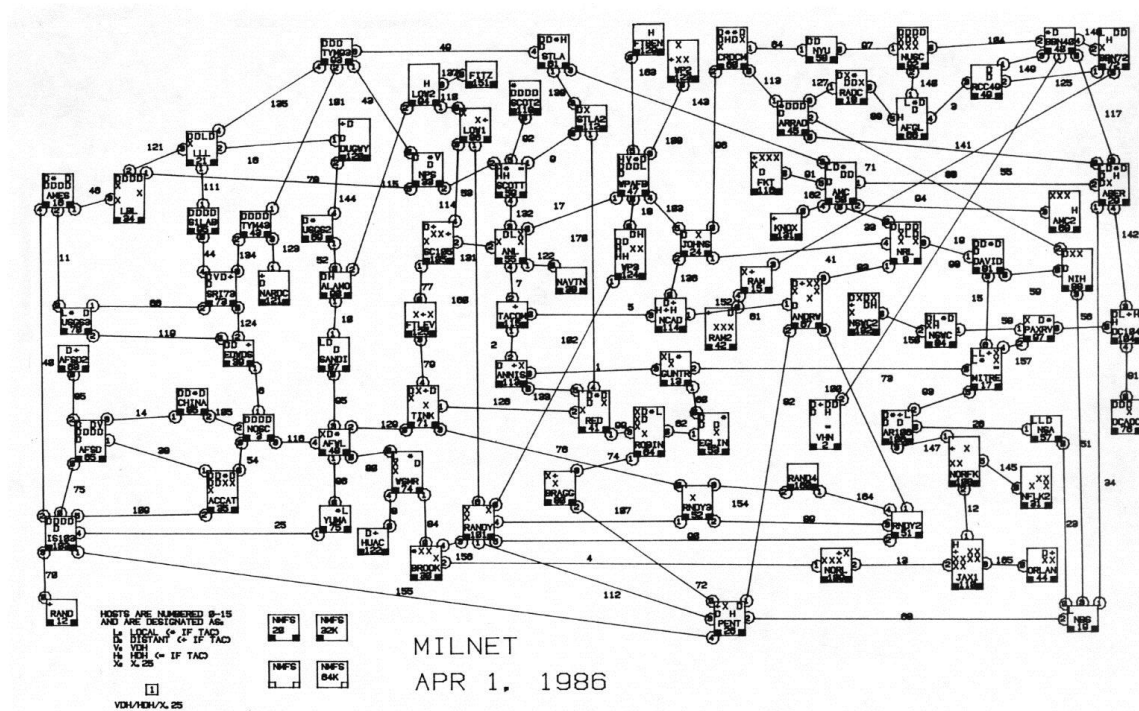
המונח **Surface Web** מתייחס לחלקים באינטרנט שניתנים למפתוח על ידי מנועי חיפוש קונבנציונליים. מנועי חיפוש בונים מאגרי מידע של הרשת בעזרת שימוש בתוכנות הנקראות Spiders או Web Crawlers שמתחילים את עבודתם עם רשימה של אתרים מוכרים. ה"עכביש" מקבל העתק של כל דף וממפתח אותו ומידע שימושי כך שיהיה נגיש במהירות לפעם הבאה שיהיה צריך לשלוח אותו. כל קישור לדף חדש בו ה"עכביש" לא ביקר, מתווסף לרשימת הדפים שאותם הוא צריך לבקר בהמשך. בסופו של דבר, כל הדפים הנגישים ממופתחים, אלא אם לעכביש נגמר הזמן או השטח בהארד-דיסק (ראוי לציין שלגוגל ו-Bing אין באמת מגבלת זמן או דיסק). אותו אוסף של דפים נגישים הוא זה שמגדיר את ה-Surface Web.

**Deep Web**, הידוע (גם בשמות Undernet, Invisible Web, Deepnet או Hidden Web) הוא החלק ברשת שאינו שייך ל-Surface Web. רבים מבלבלים בין ה-Undernet ל-Dark Internet אבל בשורות הבאות אסביר את ההבדלים ביניהם. Mike Bergman, מייסד חברת BrightPlanet טבע את המשפט הבא: "ניתן להקביל חיפוש באינטרנט כיום לגרירה של רשת דיג באוקיינוס. דברים רבים יכולים להיתפס ברשת, אבל כמות אדירה של מידע נמצאת עמוק מאוד, ולפיכך מתפספסת".

מחקר שנערך מטעם אוניברסיטת קליפורניה שבברקלי בשנת 2001, אומד את נפח ה-Undernet בכ- 7,500 טרה-בייטס. הערכות נוספות מדברות על מספרים כמו כ-300,000 אתרים כל ברחבי ה-Undernet בשנת 2004 וכ-14,000 אתרים בחלק הרוסי של ה-Undernet בשנת 2006.

אחרון (ולא) חביב - **Dark Web** הוא מונח שכולל בתוכו את כל הרשתות באינטרנט שאינן נגישות. אין לבלבל בין ה-Dark Web לבין ה-Undernet שכן האחרון מתייחס לרשתות סודיות ואתרים שקשה למצוא בעוד הראשון כבר לא נגיש באמצעים קונבנציונליים. כישלונות בהקצאת משאבים אינטרנטיים שנוצרו בשל מגמת הצמיחה הכאוטית של האינטרנט הן הסיבה העיקרית להיווצרות ה-Dark Internet. צורה אחת של Dark Internet היא אתרים צבאיים שיושבים ב-MILNET הארכאית.

MILNET (קיצור של Military Network) היא שם שניתן לחלק ב-ARPANET המיועד לתעבורת רשת בלתי מסווגת של משרד ההגנה האמריקאי. בשנת 1983 פוצלה ה-MILNET מה-ARPANET שנשארה שמישה לטובת מתן שירותים לקהילת המחקר האקדמי. הקישוריות הישירה שהייתה קיימת בין שתי הרשתות נחתכה מסיבות אבטחה. מאוחר יותר בשלהי שנות ה-80 התרחבה והפכה ל-DDN (Defense Data Network) שבסופו של דבר הפכה בשנות ה-90 ל-NIPRNET (קיצור של Non-classified Internet Protocol Router Network) בעשורים האחרונים גדלה ה-NIPRNET לממדים אדירים וכיום היא מהווה את הרשת הפרטית הגדולה בעולם. עובדה זו מקשה מאוד על משרד ההגנה האמריקאי לבצע בקרה ומדי שנה 10 מיליון דולרים מהתקציב האמריקאי הולכים לטובת מיפוי של המצב העדכני של הרשת, במאמץ לנתח את התפתחותה ולזהות משתמשים שאינם מורשים. חלק מ-10 מיליון הדולרים הללו, הולך גם לבדיקת ואיתור חולשות באבטחה. בשנים האחרונות משרד ההגנה האמריקאי עושה מאמצים כבירים לשיפור האבטחה של הרשת ובשנת 2012 הפנטגון הודיע כי הוא מבקש 2.3 מיליארד דולרים על מנת לשדרג את האבטחה.



[תרשים של ה-MILNET מה-1 באפריל 1986]

כעת נחזור לעניננו. גילן של הרשתות הממשלתיות הללו הוא לפעמים שווה ערך לגיל ה-ARPANET המקורי, ולפעמים הן בדיוק אותן רשתות ממשלתיות פשוט לא התאגדו לתוך ארכיטקטורת האינטרנט שבינתיים התפתחה. על פי מקורות מסוימים, קראקרים משתמשים בטכניקות שונות לחטיפת ראוטרם פרטיים על מנת שיוכלו לנתב דרכם תקשורת או להסוות פעילות שאיננה חוקית. בעזרת שימוש בראוטרם הפרטיים הללו, ה-Dark Web יכול לשמש כפלטפורמה לשימוש פסול באינטרנט.

אז לסיכום, כדי לחדד את ההגדרה של ה-Dark Web, מדובר בחלק באינטרנט שמורכב ממכונות שאינן נגישות באמצעים קונבנציונליים. לרוב המשמעות היא שהגדרות בראוטר כווננו כך שלא יהיה ניתן לגשת אליו. עם זאת, הביטוי "אין נגישות" משתנה בעיני המתבונן. בסופו של דבר מחשבים שנמצאים ב-Dark Web עדיין מחוברים, פשוט לא ניתן לגשת אליהם בשיטות ה"מסורתיות".

כדי לקבל סדר גודל לגבי ההבדלים בין ה-Undernet ל-Surface Web מצורפת הטבלה הבאה:

Surface Web	Undernet
מיליוני דפי אינטרנט	מעל ל-200,00 בסיסי נתונים
כמיליארד מסמכים	כ-550 מיליארד מסמכים
19 טרה-בייטס	כ-7,750 טרה-בייטס
תוצאות מכילות פרסומות	ללא פרסומות

## מי מתעניין ב-Undernet ולמה?

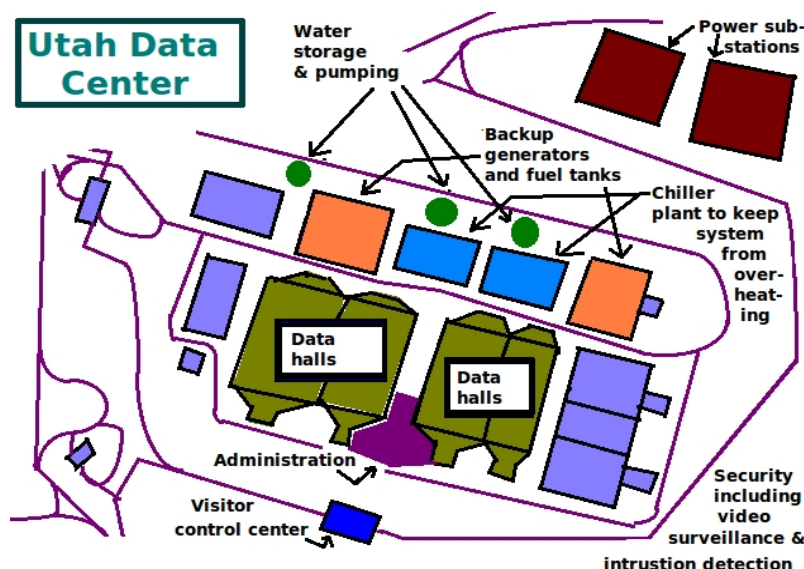
אנונימיות היא צורך קיומי עבור פושעי סייבר ולאורך השנים התפשטו ופותחו טכנולוגיות שונות שמיועדות לשמר את האנונימיות ברשת. החל בכאלה שמצפיות ערוצי תקשורת של מסרים מידיים (דוגמת PGP) וכלה בשירותי VPN. ה-Undernet מספקת לגולשים בה הזדמנות לחמוק מעיניהם של אלה שאוכפים את החוק. פושעי סייבר מאופיינים בכך שישות טכנית כלשהי משתמשת בשירותים החבויים ב-Undernet. ב"שוק השחור" סוחרים יכולים להקים מכירות פומביות, למכור תוכנות זדוניות ופרצות Zero-Day תוך שימור האנונימיות של כל הגורמים המשתתפים במכירה. מלבד פושעי סייבר, גם עיתונאים משתמשים בשירותי ה-Undernet בכדי לעקוף את הצנזורה של מדינות מסוימות.



ומי עוד מתעניין ב-Undernet?

מטבע הדברים, ממשלות מגדילות את היכולת שלהם לפקח על הרשת החבויה. לאחרונה ה-FBI הקים יחידת מעקב שתפקידה הוא לפתח כלים טכנולוגיים לפיקוח על האינטרנט ועל תקשורת אלחוטית. "Going Dark" הוא שם הקוד לפרויקט שמרחיב את היכולות של ה-FBI ובכך מספק להם את היכולת להאזין לתקשורת בזמן אמת. על פי מקורות מסוימים, ל-FBI כבר יש יכולת ליירט הודעות ברשתות חברתיות וגם אימיילים. סביר מאוד להניח שחלקכם שמע על המערכת הזו שידועה בשם [Carnivore](#) ומאוחר יותר שמה שונה ל-DCS1000.

בדומה ל-FBI, גם ה-NSA משקיעה משאבים בניטור של הרשת. לפני כשנה, הסוכנות החלה לבנות את מרכז הריגול הגדול ביותר בעיר Bluffdale. המרכז נקרא [Utah Data Center](#) ותפקידו יהיה ככל הנראה לנטר, לפענח ולעבד כל תקשורת שנמצאת תחת חקירה, מבלי להתחשב בסוג השידור. עלות המרכז היא כ-2 מיליארד דולר והוא צפוי להפוך למבצעי בספטמבר 2013.



[Utah Data Center - תרשים מתוך Wikipedia]

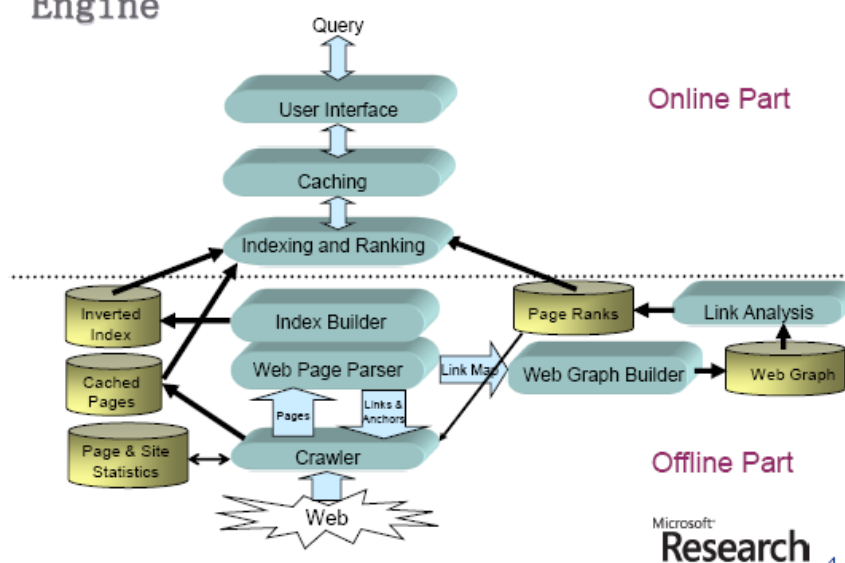
עם זאת, למרות כל מה שכתבתי לעיל, צריך להדגיש שב-Undernet משתמשים גם מדענים, חוקרים, עיתונאים ואנשים נורמטיביים שפשוט רוצים לשמור על הפרטיות שלהם.

## מדוע חלק מהמידע לא נגיש למשתמש הממוצע?

מנועי חיפוש "רגילים" אוספים את המידע בשתי דרכים עיקריות:

1. קבלת המידע מ-Web Master (בעל האתר) אשר מעוניין כי האתר שלו יופיע במנוע החיפוש.
2. שימוש בתוכנות שנקראות "Crawlers" או "Spiders". אלה תוכנות שמסיירות ב-WWW בדומה לגולש אבל באופן מתודי ואוטומטי ומיועדות ליצור העתק של כל הדפים בהן הן ביקרו, ומשם יועברו לעיבוד על ידי מנוע החיפוש שימפתח את הדפים שהורדו בכדי לאפשר חיפושים מהירים.

### Architecture of a Typical Search Engine



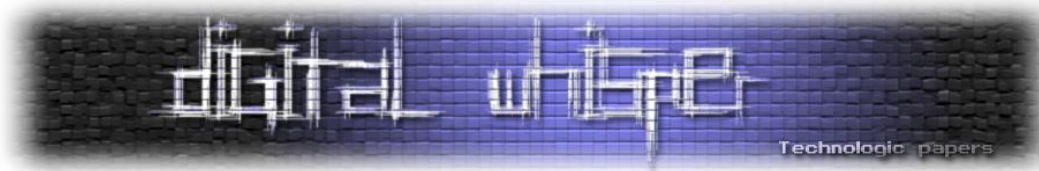
[במקור: [http://www2.hawaii.edu/~chenx/reading/crawler/search\\_engine\\_arch.PNG](http://www2.hawaii.edu/~chenx/reading/crawler/search_engine_arch.PNG)]

לעוד מידע על כיצד מנועי חיפוש עובדים, ניתן לקרוא את ערך הנושא בויקיפדיה:

[http://en.wikipedia.org/wiki/Web\\_crawler](http://en.wikipedia.org/wiki/Web_crawler)

הטכניקה הנ"ל טובה, אך לא יעילה למציאת משאבים שנכנסים לאחת מהקטגוריות הבאות:

1. תוכן דינאמי - דפים דינמיים שמחזירים תשובה כשנשלח אליהם קלט, או כאלה שניגשים אליהם דרך טפסים (Forms).
2. תוכן לא מקושר - דפים שלא מקושרים אל דפים אחרים, בצורה כזו שמונעת מה-Crawlers/Spiders להגיע אליהם. דפים כאלה נקראים Backlinks או Inlinks.
3. דפים פרטיים - אתרים שדרושים הרשמה ולוגין.



4. דפי תוכן הקשרי - כאלה שהתוכן שלהם משתנה בהתאם למחשב שניגש אליהם. (לדוגמא, גישה מכתובת IP XXX.XXX.XXX.XXX תציג דף מסוג Y).
5. תוכן מוגבל גישה - אתרים שמגבילים את הגישה אליהם באמצעים טכניים כמו Robots.txt, CAPTCHAs וכו'...
6. תוכן שהוא Scripted - דפים שניתן לגשת אליהם רק דרך קישורים שנוצרים ב-JavaScript. כמו כן, תוכן שמורד בצורה דינאמית משרת ה-Web דרך Flash או Ajax.
7. תוכן שאיננו HTML/Text - טקסטים שמוטמעים בתוך מולטימדיה (תמונות/וידאו) או קבצים בפורמט שלא נתמך על ידי מנועי החיפוש.
8. תוכן טקסט בפרוטוקול Gopher וקבצים שמאוחסנים על שרתי FTP שלא "מסומנים" על ידי רוב מנועי החיפוש. Google לדוגמא לא "מסמנת" אתרים מחוץ לפרוטוקולים HTTP או HTTPS.

### איך לשפר את האופן בו אנחנו מחפשים מידע באינטרנט?

נסו לחשוב ב"מסדי נתונים" ופתחו את העיניים שלכם. תוכלו למצוא מסדי נתונים שלמים שמכילים דפים מה-Undernet על ידי חיפוש שגרתי ברוב ספריות ה-Web הכלליות:

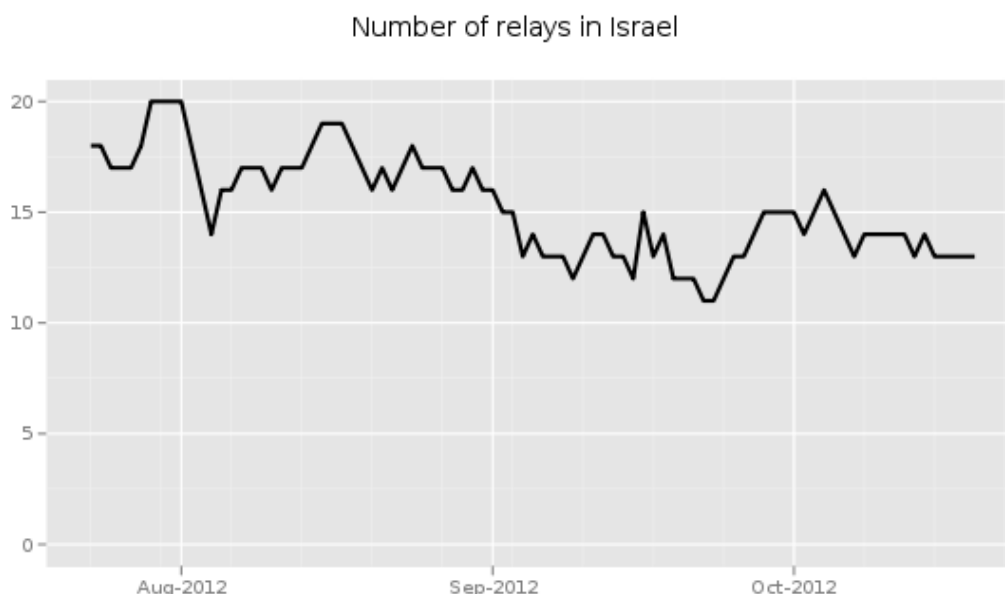
ipl2 (www.ipl.org)	Infomine (infomine.ucr.edu)	About.com (www.about.com)	!Yahoo (dir.yahoo.com)	
מעל ל-40,000 רשומות. אך ורק אתרים באיכות גבוהה. שימושי ואמין. מיזוג בין אינדקס האינטרנט של הספרנים והספרייה הציבורית של האינטרנט	מעל ל-125,000 רשומות, שימושי ואמין. עובד על ידי ספרנים אקדמיים מאוניברסיטת קליפורניה	מעל ל-2 מיליון רשומות	כ-4 מיליון רשומות, תיאורים מאוד קצרים, שימושי בעיקר לנושאים מסחריים	<b>גודל / סוג</b>
לא	כן, צריך להשתמש ב-" "	כן, צריך להשתמש ב-" "	כן, צריך להשתמש ב-" "	<b>קיים חיפוש מדויק?</b>
AND, OR, NOT	AND, OR, NOT	לא	כן, בדיוק כמו במנוע החיפוש הרגיל של יאהו!	<b>קיום ביטויים לוגיים?</b>

טיפ: השתמשו בגוגל ובמנועי חיפוש אחרים בכדי לאתר מסדי נתונים על ידי חיפוש המילה "database". זכרו שה-Undernet קיימת. בנוסף למה שאתם מוצאים במנועי החיפוש (כולל Google Scholar) ותיקיות Web- בטבלה הנ"ל, ישנם "מכרות זהב" נוספים בהם תצטרכו לחפש. מכרות אלה כוללים מגזינים, ארכיוני חדשות ועוד מגוון מקורות שמכוני מחקר וספריות משלמים כסף בכדי לחפש בהם.

### ה-Undernet בתור כלי ניתוח עוצמתי

עד כה ראינו שה-Undernet, בזכות האנונימיות שהיא מספקת, פותחת הזדמנויות למגוון פושעי סייבר, אבל מלבד זאת היא יכולה להוות גם כלי ניתוח שימושי. Tor Metric Portal מציע ניתוחים סטטיסטיים שמייצגים את נפח הפעילות ב-Tor. ערכים אלה יכולים לשמש גם למטרות מודיעין. לדוגמא, אם ננתח מדדים עיקריים ברשת נוכל ללמוד על קיומן של מערכות ניטור פנים-ארציות למטרות צנזורה. לאחרונה, נעשה שימוש במערכות שכאלה באיראן ובסוריה בניסיון לדכא מחאות של מתנגדי המשטר ודליפה של מידע אל מחוץ למדינה. מצבים אלה הם ביטוי של משבר פוליטי במדינה ושימוש נכון ב-Tor Metric Portal יכול לתת אלמנט נוסף של הערכה לניתוחים המודיעיניים של חוקרי המודיעין.

לדוגמא, ניתוח של מספר הגישות לרשת Tor בהצלבה עם "כמה גישות היה ניתן לבצע ל-Tor באותו זמן", מגלה לנו איך תאגיד הטלקומוניקציה האתיופית פרס למטרות בדיקה (Packet Inspection Deep) DPI על כל תעבורת האינטרנט במדינה.



The Tor Project - <https://metrics.torproject.org/>



## איך מגיעים לחלקים עמוקים יותר ב-Undernet?

על מנת לגשת לחלקים עמוקים יותר ב-Deep Web, צריך להשתמש ב-Proxy כמו Tor.

בחיי היום-יום שלנו יש לנו רמה מסוימת של פרטיות. יש לנו וילונות על החלונות, דלתות למשרדים ואפילו מגני מסך מיוחדים ש"חוסמים" עיניים סקרניות. הרצון לפרטיות מתרחב גם לשימוש באינטרנט. אנחנו לא רוצים שאנשים ידעו מה כתבנו בגוגל, על מה דיברנו בתוכנות כמו Messenger, או באילו אתרים גלשנו. לצערי, המידע הפרטי שלכם, ברובו, נגיש למי שצופה...

כשאתם עושים דברים מסוימים באינטרנט, קיימות סיבות רבות למה תרצו להישאר בעילום שם. עם זאת, זה לא בהכרח אומר שאתם עושים משהו לא חוקי.



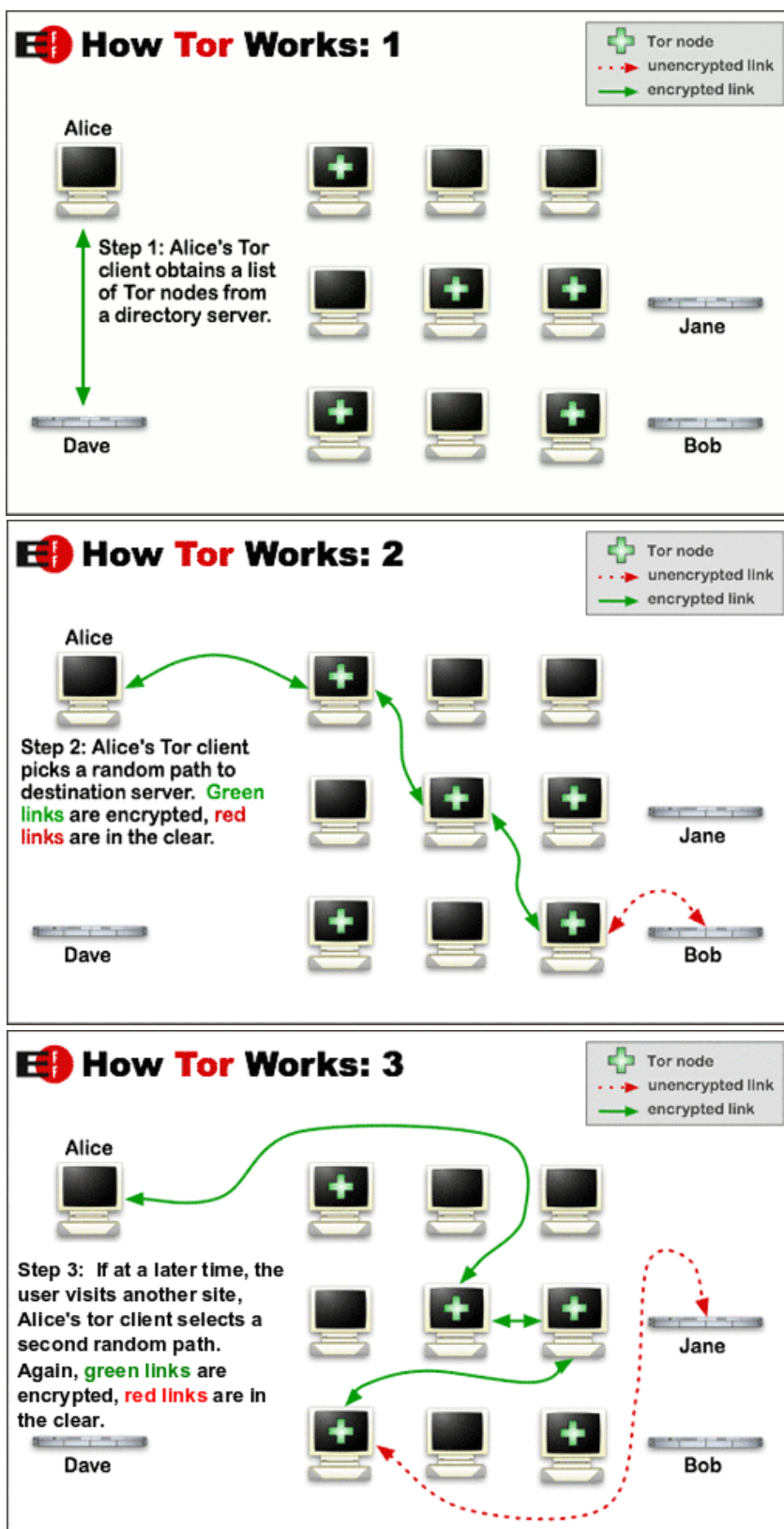
פרויקט Tor, ראשי תיבות של The Onion Router הוא פתרון מוכר לבעיית הפרטיות באינטרנט. לפרויקט יש היסטוריה ארוכה שנובעת מפרויקט שנוהל על ידי מעבדת מחקר של הצי האמריקאי. לאלו שמתעניינים בהיסטוריה, תוכלו למצוא עוד חומר כאן:

<http://www.torproject.org>

Tor היא בעצם רשת של מחשבים מסביב לעולם אשר מעבירה בקשות באופן מוצפן מתחילת הבקשה ועד שהיא מגיעה למכונה האחרונה ברשת, הידועה גם בתור exit node. בנקודה זו, הבקשה מפוענחת ומועברת אל שרת היעד. Exit node משמשת גם כנקודת היציאה של הבקשה וגם בתור נקודת הכניסה למידע שחוזר למשתמש שהגיש את הבקשה.

כאשר אתם משתמשים ב-Tor, היעד הסופי שאיתו אתם מתקשרים, רואה את התקשורת הנכנסת כאילו מקורה מה-exit node. הוא לא יודע איפה אתם נמצאים או מהי כתובת ה-IP האמתית שלכם. יתר על כן, המערכות האחרות ברשת Tor אינן יכולות לדעת את המיקום שלכם, מכיוון שבסופו של דבר הן רק מעבירות תנועה מבלי לדעת מה מקורה. התקשורת שתחזור אליכם בתגובה תגיע אליכם אבל מבחינת Tor אתם בסך הכל עוד "הופ" בדרך.

תרשים שמפשט את Tor (לקוח מהאתר של Tor)



תוכנת Tor היא חנימית לשימוש וזמינה לרוב מערכות ההפעלה. תוכלו להתקין את Tor על מערכת ה-Ubuntu שלכם על ידי כתיבת הפקודה: `apt-get install tor`. לפלטפורמות אחרות כמו Windows או Mac OS X תוכלו להוריד את החבילה מהאתר של Tor. ברוב המקרים, מה שתמצאו להוריד זה את ה-Bundle.

ניתן להוריד מכאן:

<https://www.torproject.org/download/download>

לאחר ההתקנה, תוכלו להשתמש מידית ב-Tor. שימו לב שאם תורידו את ה-Bundle, כל התעבורה של הדפדפן שלכם תעבור דרך Tor. אם ברצונכם להשתמש בדפדפן אחר כמו Firefox, הדבר אפשרי ופשוט יחסית לביצוע. כל שעליכם לעשות הוא להתקין "הרחבה" ל-FireFox שנקראת TorButton.



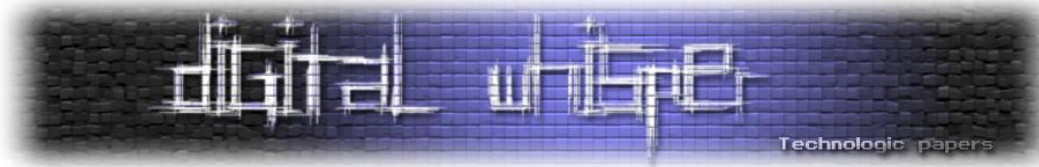
הכפתור נמצא בפינה הימנית למטה של הדפדפן מרגע שההרחבה מותקנת. לחיצה פשוטה על הכפתור מאשרת לכם להפעיל או לכבות את השימוש ב-Tor. כעת כל שנתר לכם לעשות זה לקנפג את הדפדפן שלכם כך שיעבוד עם ה-Proxy. בנקודה זו, אתם אמורים להיות מסוגלים לגלוש באינטרנט באנונימיות. בכדי לוודא שהפעילות שלכם אכן אנונימית כדאי להיכנס לאתר כמו <http://www.whatismyip.org> ולוודא שכתובת ה-IP שחוזרת אליכם מהאתר שונה מכתובת ה-IP האמתית שלכם. אם זה המצב, הכל עובד כמו שצריך ותוכלו להמשיך בעסקיכם.

## המגרעות של Tor

בעוד Tor היא שירות מעולה, יש לה גם חסרונות. חסרונות אלו ישפיעו על מהירות הגלישה שלכם, האבטחה והאמינות של מידע שנשלח על גבי הרשת והיכולת שלכם לגשת למשאבים.

1. מהירות - החיסרון העיקרי של Tor הוא מהירות הגלישה האיטית. זוהי בעיה מוכרת והיא קיימת מכמה סיבות. החיבור שלכם מקפץ בין מדינות בכל רחבי העולם, ובנוסף, חלק מעמדות ה-Tor הן בעלות רוחב-פס נמוך. למזלנו, קיימות תכניות לשדרוג המהירות והביצועים של Tor.

2. מפעילי Tor בלתי-מהימנים - אנשים חסרי מצפון ידועים בהרצה של exit nodes. מה זה אומר? המשמעות היא שמפעיל Tor שרץ על exit node ומסתכל באופן ספציפי על התקשורת שלכם, יכול לשנות את התנועה לרווחתו. אם אתם מבצעים Login לאפליקציה שאינה משתמשת ב-SSL להצפנת



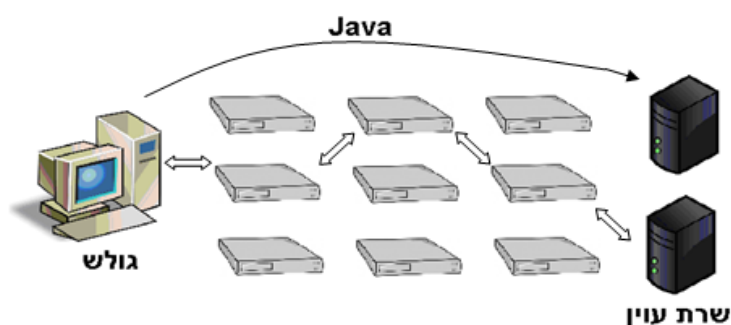
הסיסמא, הפרטים שלכם חשופים לעיניו של מפעיל exit node. כמו כן, קחו בחשבון שמפעילי exit nodes מסוגלים לבצע מגוון מתקפות כמו man-in-the-middle ואפילו להזריק תקשורת ל"שיחות" שאינן מוצפנות. לדוגמא, דמיינו שאתם גולשים באתר אינטרנט רגיל, ומישהו שמפעיל exit node מחליט להזריק לכם iframe או קוד JavaScript זדוני. אם הקוד מנסה לנצל חולשה שהמחשב שלכם פגיע בפניה, אתם עלולים למצוא את עצמכם נגועים.

3. רשימות שחורות - אתרים ושירותים מסוימים באינטרנט עוקבים אחר התנהגותם של אלה שמפעילים exit node. המשמעות של כך היא שאתם עלולים להיחסם מגישה לאתרים מסוימים בזמן השימוש ב-Tor. בעוד שרוב השימוש ב-Tor הוא לגיטימי, אנשים מסוימים משתמשים ב-Tor בכדי להחביא פעילות לא-חוקית. כתוצאה מכך, אתרים מסוימים בוחרים לחסום גישה לכתובות IP מסוימות כדי לצמצם את אותה פעילות.

## מתקפות ברשת Tor

אם כבר התחלנו לגעת במגרעות של Tor זה יכול להיות זמן מתאים לדבר על כמה מתקפות פוטנציאליות כנגד משתמשי Tor. באופן כללי ניתן לומר ש-Entry node היא המערכת היחידה שיודעת את הזהות האמיתית של "הלקוח" ו-Exit node היא המערכת היחידה שיודעת את היעד של "הלקוח" ומהו המידע שהוא שולח.

1. **מתקפה דרך Plug-Ins בדפדפן** - בכדי לגלוש באנונימיות דרך Tor, "הלקוח" חייב להשתמש ב-HTTP Proxy כך שהמידע שלו יעבור דרך Tor ולא על גבי האינטרנט. יש לכך חשיבות מרובה מכיוון שברירת המחדל של דפדפנים היא לשלוח שאילתות DNS שלא דרך SOCKS. גם אם משתמשים ב-Tor, אתרים מסוימים יוכלו לזהות את הגולש על ידי תוספות/PlugIns שמותקנים בדפדפן שלו, לדוגמא: Flash, JAVA, בקרי ActiveX ועוד לא בהכרח מעבירים את המידע דרך ה-Proxy:



מה שאנחנו רואים בתרשים הנ"ל הוא מתקפת דפדפן שמתבצעת על ידי אפליקציית Java שכלולה באתר. במצב כזה, הדפדפן של הגולש פותח גם קשר ישיר מול מכונה שאוגרת את המידע שנשלח ועל ידי כך מסכנת את האנונימיות של הגולש.

2. **מתקפה על ידי ניצול של TorButton** - כאמור, TorButton היא הרחבה שמאפשרת למשתמש בה להפעיל/לכבות את השימוש ב-Tor על ידי לחיצת כפתור פשוטה. במתקפה הנ"ל Exit node זדוני משנה את הדפים שאליהם נכנס הגולש על ידי שתילה של קוד JavaScript שמתחבר שוב ושוב לשרת שאוגר מספר ID. אם הגולש מכבה את השימוש ב-Tor על ידי לחיצה על TorButton אבל משאיר לשוני/חלון שבו הקוד עדיין רץ, הוא יתחבר ישירות לשרת האוגר.

בפועל מדובר בהתקפה די פשוטה אבל מוגבלת באפקטיביות שלה. היא תוכל לחשוף רק גולשי Tor שיפסיקו את השימוש ב-Proxy בזמן שהדפדפן עדיין פתוח. ניתן להתגונן מההתקפה הזו בקלות אם נשנה את ההגדרות של TorButton כך שברגע שנפסיק את השימוש ב-Tor טעינה מחדש של דפים והרצה של קוד JavaScript מופסקים לפני שינוי הגדרות ב-Proxy.



3. **מתקפת MitM (Man in the Middle)** - זוהי היא מתקפה בה מידע שנשלח בין מחשב א' למחשב ב' מיורט על ידי מחשב ג' מבלי שא' או ב' יודעים מכך.

ברגע שחיבור ה-TCP מיורט, התוקף בעצם משרת כ-Proxy שמטבע הדברים יכול לקרוא ולשנות את המידע שמיורט. הסכנה ב-Tor היא מה-Exit nodes שבעצם יכולים לראות את המידע שאנחנו שולחים ליעד מבלי שהוא מוצפן. בכדי להתגונן מפני התקפה שכזו עלינו להשתמש בהצפנה חזקה **מקצה-לקצה** וכאמצעי הגנה נוסף לוודא את האותנטיות של השרת שאיתו אנחנו מדברים. תהליך האימות נעשה בדרך כלל באופן אוטומטי על ידי כך שהדפדפן שלכם משווה את תעודת ה-SSL אל מול קבוצה נתונה של רשויות אישורים מוכרות. אם אתם מקבלים הודעה בסגנון של התמונה הבאה, יכול להיות מאוד שאתם נתונים למתקפת MitM ואל לכם להתעלם מן ההודעה.



שימו לב שכדאי לקחת בחשבון את העובדה שתוקף יכול לנקוט אמצעים נוספים בכדי להביא למצב שבו ההודעה הזו תהיה "שקופה למשתמש". תמיד כדאי לצאת מנקודת הנחה שכשאתם גולשים ב-Tor המידע שאתם מעבירים עלול להיות גלוי למישהו.

4. **תחנות Tor בבעלות עוינת** - לא ניתן להוכיח זאת, אך מספר רב של חוקרי אבטחה עם שם עולמי בתחום דוגלים בהנחה כי מספר רב של Exit Nodes נמצאים בבעלות גופים עם מטרות לא תמימות (כגון ה-NSA). הרעיון הוא שבמידה ולגוף יהיה שליטה על כלל החוליות (כברירת מחדל - 3) המהוות את תחנות המסר של חבילת מידע ובייחוד על תחנת הקצה (ה-exit node) ניתן יהיה להבין רבות על הגולש.

עד כאן עם מתקפות שניתן לבצע על משתמשי Tor. יחד עם זאת, ראוי לציין שקיימות מתקפות אפשריות רבות נוספות.



## לסיכום

גלישה ב-Deep Web יכולה להיות מעניינת ופרודוקטיבית אך יחד עם זאת גם מסוכנת. לפעמים מספיקה בקשה אחת משרת בכדי לחשוף אתכם ואת המידע שאתם שולחים. כשאתם נרשמים לשירותים כלשהם, אל תשתמשו בשמות שמזהים אתכם או את הארגון שלכם. בנוסף, אל תשתמשו בסיסמאות שבהן אתם משתמשים בחשבונות אחרים שלכם. אם אתם נתקלים במשהו שנראה לכם מפוקפק (וסביר להניח שתתלו בכזה) או שאתם מבצעים פעילות שאתם חוששים ממנה למרות היותכם אנונימיים, עליכם להפסיק.

## על המחבר

דן פלד (26) הינו סטודנט לניהול ומדעי המחשב באוניברסיטה הפתוחה ומחזיק בתעודת CEH. עולם אבטחת המידע ותחום הסייבר ריתקו, מרתקים ומעסיקים את דן מאז שהיה ילד, עובדה שהפכה אותו לבעל ידע רב בתחום. את שירותו הצבאי העביר דן ביחידת מודיעין של חיל האוויר וכיום הוא משקיע את רוב זמנו בלימודים.

## לקריאה נוספת

<http://www.digitalwhisper.co.il/files/Zines/0x07/DW7-4-TORAnalyzing.pdf>

<http://www.binaryvision.org.il/?p=988>

<http://www.binaryvision.org.il/?p=1002>

[http://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008\\_37.pdf](http://homes.cs.washington.edu/~yoshi/papers/Tor/PETS2008_37.pdf)

## רשימת מקורות

<http://en.wikipedia.org/>

[http://www.teamliquid.net/forum/viewmessage.php?topic\\_id=229525](http://www.teamliquid.net/forum/viewmessage.php?topic_id=229525)

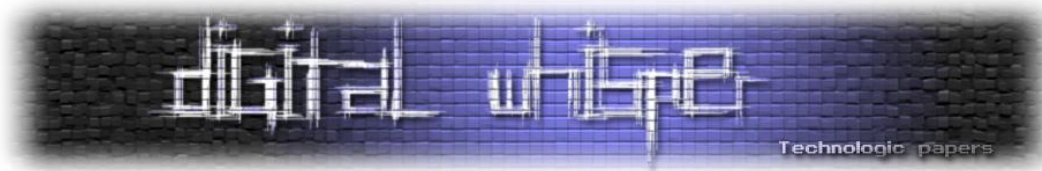
<http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html>

<http://oak.cs.ucla.edu/~cho/papers/ntoulas-hidden.pdf>

---

המדריך לתייר בסמטאות האפלות של הרשת

[www.DigitalWhisper.co.il](http://www.DigitalWhisper.co.il)



<http://ilpubs.stanford.edu:8090/456/1/2000-36.pdf>

<http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf>

<http://securityaffairs.co/wordpress/9409/security/the-deep-web-part-1-introduction-to-the-deep-web-and-how-to-wear-clothes-online.html>

<http://www.worldwidewebsize.com/>

<http://cyberwarzone.com/cyberwarfare/attacking-tor-network>

<http://gizmodo.com/5927379/the-secret-online-weapons-store-thatll-sell-anyone-anything>

<https://tails.boum.org/doc/about/warning/index.en.html>

<http://www.orkspace.net/secdocs/Conferences/BlackHat/USA/2007/Securing%20the%20Tor%20Network-paper.pdf>

<http://www.mit.edu/~ecprice/papers/tor.pdf>

<http://webapps.lsa.umich.edu/lsait/admin/TOR%20Routing%20Infomation%20.pdf>

[www.thehackernews.com](http://www.thehackernews.com)