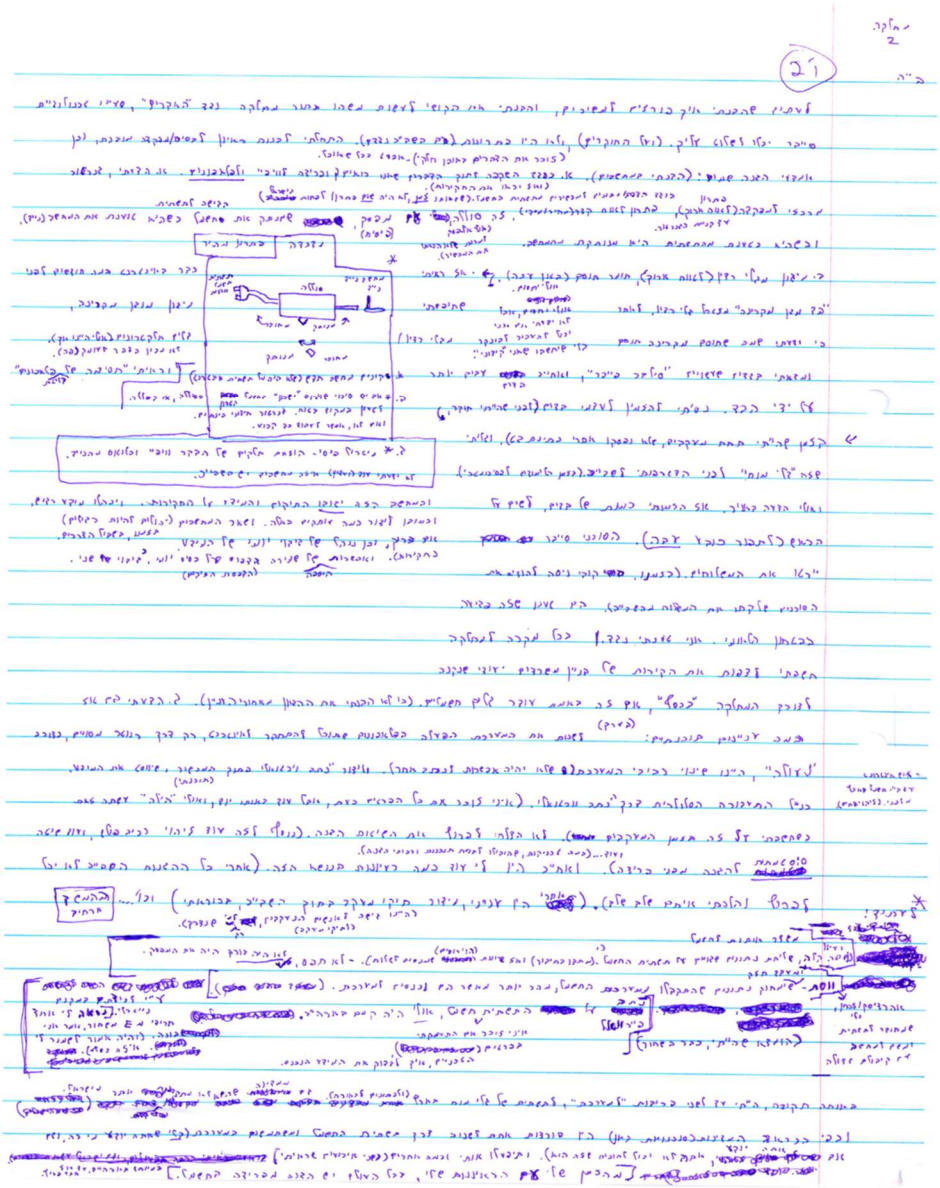


ו' – 2

ב"ה מחלקה 2

לעתיד שהבנתי איך פורצים למכשירים, והבנתי את הקושי לעשות משהו בתור מחלקה נגד "האקרים", שע"י טכנולוגיית סייבר יכלו לשלוט עליך (ועל החוקרים), ולא היו פתרונות (גם בשב"כ נגדם). התחלתי לבנות רעיון לבסיס/מפקדה מובנת, וכן אמצעי הגנה שונים: (הבנתי במחשבים). א. כנגד השקפה לתוך הדברים שאנו רואים ופריצה לווייפיי ולפלאופנים. א. הצעתי גנרטור מרכזי למפקדה (פתרון לטווח ארוך עם קניית הגנרטור), כנגד הצפת נתונים למכשירים מתשתית החשמל. (שבאותו זמן, לא היה שום פתרון לפחות בישראל). פתרון לטווח קצר (מהיר/ מיידי) זה סוללה (אולי אל-פסק למרות שלא הכרתי את המכשיר), עם מפסק(פיסית), שמנתק את החשמל כשהיא טוענת את המחשב (נייד), וכשהיא נטענת מהתשתית היא מנותקת מהמחשב. ב. מיגון מגלי רדיו (לטווח ארוך), חומר חוסם (בטון עבה אולי יחסום). אולי יחסום אבל לא ידעתי אם אני יכול להעביר לבונקר בלי שיחשבו שאני "קיצוני". אז ראיתי כבר באינטרנט כמה חודשים לפני "בד מגן מקרינה" מנטרל גלי רדיו, לאחר שחיפשתי מיגון מגן מקרינה, כי ידעתי שמה חוסם מקרינה חוסם מגלי רדיו/גלים אלקטרוניים (אולי היינו אך לא נכון בדבר העומק (פה), ומצאתי בגדים שעשויים "סילבר סייבר", ואח"כ בדים עבים יותר וראיתי "חסימה של קליטת פלאפונים" על ידי הבד. ניסיתי להזמין לעצמי בדים (לפני שהייתי חוקר, בזמן שהייתי תחת מעקבים שלא פסקו אחרי נתינת הגט), וגיליתי שזה "גלי מוח" לפני הצטרפותי לשב"כ. (בזמן הלימודים לפסיכומטרי). ואולי הצעה באוויר. אז הזמנתי כמות של בדים, לשים על הראש (לתפור כובע עבה). סוכני הסייבר יירטו את המישלוחים (בזמנו, קובי ניסה להוציא את הסוכנים שלקחו את המשלוח מהשב"כ). הם טענו שזו פגיעה בביטחון הלאומי. אני טענתי נגד. בכל מקרה למחלקה חשבתי לצפות את הקירות של בניין משרדים ייעודי שנקנה לצורך המחלקה "בכסף", אם זה (בערך) באמת עוצר גלים חשמליים. (כי לא הבנתי את ההגיון מאחורי העניין). ג. הצעתי גם אז כמה עניינים תוכנתיים: לשנות את מערכת ההפעלה בפלאפונים שתוכל להתחבר לאינטרנט, רק דרך ראוטר מסוים, בצורה "נעולה", דהיינו שינוי רכיבי המערכת (שלא תהיה אפשרות לנתב אחר). וליצור נתב וירטואלי (תכנתי) בתוך המכשיר, שיווסת את המידע, כנ"ל התעבורה הסלולרית דרך הנתב הווירטואלי. (איני זוכר את כל הפרטים כעת, אבל עוד באותו יום, ואולי "הילה" עשתה זאת כשחשבתי על זה בזמן המעקבים, לא הצליחו לפרוץ את השיטות הגנה. (נוסף לזה עוד זיהוי רכיב פולש, ועוד שיטה סיסטמתית להגנה מפני פריצה). ועוד... כמה טכניקות שהובילו לבניית תוכנות ורכיבי הגנה. ואח"כ היו לי עוד כמה רעיונות בנושא הזה. (אחרי כל ההגנות השב"כ לא יכול היה לפרוץ והלכתי איתם שלב שלב). (אחרי היו ענייני מידור תיקי מעקב בתוך השב"כ, בהוראתי) וכו'... (בהמשך ארחיב) (היינו גישה לאנשים (לתיקי מעקב) שבמעקב, רק למי שנצרך).

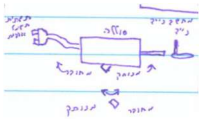
משדר אותות לחשמל. רעיון לשיטה קלה, שליחת נתונים שגויים על תשתית החשמל. (מתקן בחיבור) ואז ערמת (הוירוסים) שמנסים לשלוח) – לא תפס, לא היה צורך היה את המפסק.

ווסת – מעבד חזק שימחק נתונים שהתקבלו ממערכת החשמל, מהר יותר מאשר הם נכנסים למערכת. ע"י לכידתם במקום נייטראלי (נראה לי אחרי חרידי מ-E משחור, אמר אני הוזה. (והיה אמור לשמור לי איזה כסף).

נתב פירושו על תשתית החשמל, אולי היה קיים בארה"ב. איני זוכר אם התעמקתי בפרטים, איך לבדוק את המידע הנכנס.

* לעתיד! הארק דיסק/זיכרון כלי שמחובר לתשתית ומשם למחשב עם קיבולת גדולה.

האותה תקופה הייתי עד לשתי פריצות "למערכת", לתשתית של גלי מוח בארץ (ולנתונים לכאורה). גם ממדינה שהיא לא מתקדמת יותר מישראל. וכפי הנראה המדינות (סוכנויות ביון) היו פורצות אחת לשנייה דרך תשתית החשמל ומשתמשים במערכת (בלי שאתה יודע מי זה, וגם אם אתה יודע, אתה לא יכול להוכיח שזה הוא). ותפעלו אותי וכמה אחרים (בשני אירועים שראיתי) במיוחד בארה"ב. עד אז הכל פרוץ. (מהזמן שלי עם הרעיונות שלי, בכל העולם יש הגנה מפריצה בחשמל).



נדנדה

א. קונים מחשב חדש (שלא היה על תשתית אינטרנט).

ב. אם יש סיכוי שווירוס "ישכון" בחשמל הטעון בסוללה, או בסוללה לטעון במקום בטוח. גנרטור חיצוני בינתיים. ואם לא, אפשר לעבוד כך קבוע.

ג. ניטרול פיסי – הוצאת חלקים של הבקר ווייפיי ובלוטוס מהנייד, לא ידעתי עוד (ועדיין) איזה מחשבים יש בשב"כ.

ובמחשב הזה ייגבו את התיקים והמידע על החקירות. ינהלו מידע רגיש, וכמובן ליצור כמה עותקים כאלה. ושאר המחשבים (יכולים להיות רגישים) בזמנו, בשביל הצרכים. אם צריך, וכן נוהל של גיבוי יומי של המידע (חקירות). ואפשרות הוספה של שמירה בדפוס (הדפסת התיקים) על בסיס יומי, כגיבוי שני.