כסלו תשפ״ו
דצמבר 2025

ספרטן, תזאורוס, רוביקון, מינרבה – עלילות Crypto AG

אל״ם בדימוס דניאל רוזן

מבוא

חברת Crypto AG הייתה חברה שוויצרית שפעלה בשנים 1952 – 2018, והייתה החברה הגלובלית המובילה בתחום פיתוח וייצור ציוד הצפנה, שמכרה ציוד הצפנה למעל 120 מדינות ברחבי העולם.

בשנת 2020 התפרסם כי החברה, מהקמתה, הייתה בקשרים הדוקים עם הסוכנות לביטחון לאומי בארה״ב, NSA (National Security Agency), והגיעה עמה להסכמות לפיהן היא תמכור רק ציוד שה־NSA יודע לפענח, ולא תמכור ציוד הצפנה למדינות מסוימות. במבצע ביון שכונה 'תזאורוס', שם ששונה בשנת 1987 ל'רוביקון', החברה, שכונתה בכינוי החשאי 'מינרבה', נרכשה בחשאי בשנת 1970 בידי סוכנות הביון המרכזית של ארה״ב CIA (Central Intelligence Agency) בארה״ב ושירות הביון הפדרלי של גרמניה המערבית BND (Bundesnachrichtendienst). לאחר איחוד גרמניה באוקטובר 1990 יצא שירות הביון הגרמני מהחברה, מחשש שפעילות הריגול כנגד בנות ברית תתגלה והדבר יפגע בגרמניה, ומשנת 1993 הייתה החברה בבעלות מלאה של CIA.

גופי ביון אלה הכניסו 'סוסים טרויאניים' למנגנוני ההצפנה, וידעו לקרוא את התעבורה המוצפנת של המדינות שרכשו מהחברה את ציוד ההצפנה. המבצע סיפק ל־CIA ול־BND מידע מודיעיני רב ערך משך תקופה של עשרות שנים, ותואר כמבצע המודיעין הנועז והגדול במאה העשרים. הפרשה נחשפה בתקשורת העולמית בשנת 2020.

בין היתר, פענחו האמריקאים מסרים שהנשיא המצרי סאדאת שלח לקהיר במהלך פסגת קמפ דיויד בשנת 1977, מסרים שהעביר חומייני במהלך משבר שגרירות ארצות הברית בשנת 1979, את תעבורת צבא ארגנטינה במלחמת פוקלנד בשנת 1982 (מידע שהועבר לבריטים), סיכלו ניסיונות חיסול שתכננו דיקטטורים בדרום אמריקה, והביאו לתפיסת טרוריסטים מלוב שהוציאו לפועל פיגוע טרור בברלין בשנת 1986.

שירות הביון השוויצרי התוודע למבצע ושולב אף הוא, כשותף סוד.

פרשה זו, השתלטות סוכנויות הביון האמריקאית והגרמנית במשך עשרות שנים על התעבורה הסודית המוצפנת של מעל מאה מדינות, ידידות ויריבות, כונתה 'אירוע המודיעין של המאה'.

אנשי המפתח

שני האישים הבולטים בפרשה הם בוריס הגלין (1892–1983) [1] וויליאם (וולף) פרידמן (1891–1969), [2] ששמרו על קשרי ידידות ביניהם משלהי שנות ה־30.

[1] Boris Casear Wilhelm Hagelin
[2] William Frederick Friedman

בוריס הגלין נולד בשנת 1892 באזרבייג'ן, בן לתעשיין שבדי שניהל את שדות הנפט בבאקו עבור משפחת נובל, סיים בשנת 1914 לימודי הנדסת מכונות באוניברסיטה הטכנית בשטוקהולם, ובשנת 1922 הצטרף כמנהל הכספים לחברת ציוד ההצפנה AB Cryptograph, שהוקמה בשנת 1915, בה משפחתו השקיעה סכום ניכר יחד עם משפחת נובל. בוריס הגלין הפך להיות מנהל החברה בשנת 1925, עת החברה יצאה לשוק עם מכונת הצפנה אלקטרומכנית מתקדמת, שנקראה B-21.

בשנת 1932 נסגרה חברת AB Cryptograph ונכסיה עברו לחברת AB Cryptoteknik, בבעלותו של בוריס הגלין.

בוריס הגלין עבר משבדיה לארה"ב ב־1940, סיפק משם שירות למכונות הצפנה שנרכשו לפני המלחמה לגופי ממשל בארה"ב, ורקם קשרים אישיים עם ויליאם פרידמן ובכירים ב־CIA. הגלין חזר לשבדיה בשנת 1944.

ויליאם פרידמן נולד בשנת 1891 למשפחה יהודית בקישינב (אז – בסרביה, חלק מהאימפריה הרוסית; היום – מולדובה) והיגר עם משפחתו לארה"ב בשנת 1892, למד גנטיקה באוניברסיטה של פיטסבורג ובאוניברסיטת קורנל, ועם הצטרפות ארה"ב למלחמת העולם הראשונה התנדב למחלקת הצפנים הממשלתית Department of Codes and Ciphers. בשנת 1918 הצטרף למפקדת חיל המשלוח האמריקאי בצרפת, שם עסק בפענוח צפנים של צבא גרמניה. השתחרר מהצבא בשנת 1919. בשנת 1921 התמנה, כאזרח, לאנליסט הצפנים הראשי של משרד המלחמה (Chief Cryptanalyst for the War Department) ובהמשך ניהל את ה־SIS (Signal Intelligence Service), משנת 1949 ניהל את מחלקת הצופן ב־AFSA (Armed Forces Security Agency) ומשנת 1952 היה אנליסט הצפנים הראשי (Chief Cryptologist) של הסוכנות לביטחון לאומי NSA.

פרידמן התפרסם לא רק בשבירת צפנים גרמניים ויפניים, אלא גם כחלוץ בפיתוח שיטות מדעיות ומתמטיות לקריפטולוגיה, ופרסם ספרות מקצועית ששימשה דורות רבים. לעבודתו הייתה השפעה רבה על תחום ההצפנה ופענוח צפנים.

כהוקרה על פועלו הייחודי, נשיא ארה"ב הרי טרומן העניק לפרידמן את עיטור המופת האזרחי (Medal for Merit), ונשיא ארה"ב דוויט אייזנהאואר העניק לפרידמן את עיטור הביטחון הלאומי (National Security Medal).

ויליאם פרידמן (1891–1969)
באדיבות NSA

בוריס הגלין (1892–1983)
באדיבות Crypto AG

חברת AB Cryptoteknik

ערב מלחמת העולם השנייה התחרתה מכונת ההצפנה האלקטרומכנית B-21 תוצרת AB Cryptoteknik במכונת ההצפנה של ארתור שֶׁרְבִּיוּס (Arthur Scherbius), שהייתה הבסיס למכונת האניגמה הגרמנית.[3] שבדיה הייתה מדינה ניטרלית, שסחרה עם כל הצדדים הלוחמים.

מכונת B-21 נמכרה בגרסאות שונות – לצבא שבדיה – שעל פי דרישתו, תפעול המכשיר נעשה בדומה לאניגמה תוצרת Scherbius & Ritter, לצבא צרפת – שרכש את דגם B-211, שפעל עם אותו מנגנון הצפנה כמו B-21, אך הדפיס על סרט נייר, לברית המועצות – שהעתיקה את המוצר וייצרה בברית המועצות גרסה של B-211, עם אותיות קיריליות, בשם K-37, לגרמניה הנאצית וליפן (מכונות ההצפנה היפניות, שכונו בידי האמריקאים Red ו־Purple, היו 'הנדסה' לאחור' של מכונת B-21).[4]

חברת AB Cryptoteknik פיתחה סדרת מכשירי הצפנה אלקטרומכניים ללא סוללות (סדרה C), ובשנת 1937 מכרה לצבא ארה"ב את זכויות הייצור של מכונת הצפנה אלקטרומכנית בשם C-38, תמורת 8.6 מיליון דולר – סכום נכבד מאוד באותם הימים.

המכונה נקראה בשם M-209 ו־140,000 מכונות יוצרו בחברת מכונות הכתיבה Smith Corona בניו יורק. זו הייתה מכונת ההצפנה המובילה בדרגי השדה בצבא ארה"ב במלחמת העולם השנייה ובמלחמת קוריאה.[5]

מכונת הצפנה אלקטרומכנית B-21
מכונת הצפנה שפותחה בשנת 1925.
המכונה התמודדה מול המכונה של ארתור שרביוס, שהייתה הבסיס לאניגמה הגרמנית, ונמכרה, בגרסאות שונות, לברית המועצות, לצרפת ולשבדיה.
באדיבות Crypto AG

---

[3] דניאל רוזן, **אניגמה**, העמותה להנצחת חללי חיל הקשר והתקשוב, אב תשפ"ג – יולי 2023. ראו:
https://www.amutakesher.org.il/_Uploads/dbsAttachedFiles/Enigma_1.01.pdf

[4] האמריקאים הצליחו לפענח את התעבורה הצרפתית שהוצפנה במכונה זו (TICOM Vol. I, להלן, הערה 5, עמ' 16); גם הנאצים, האיטלקים והיפנים הצליחו לפענח את התעבורה שהוצפנה במכונה זו.
William F. Friedman, *Six Lectures on Cryptology*, NSA, 1965, NSA Ref ID: A2119475, released 30 July 2014, עמ' 163. ראו:
https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/publications/ACC15281/417851090824l2.pdf
בהרצאה שנשא בשנת 1979 (להלן, הערה 6) טען בוריס הגלין כי מכונת ההצפנה הנאצית שהייתה אמורה להחליף את מכונת האניגמה, Cipher Device 39, התבססה על מכונות מתוצרתו, וכי הוא מכר לנאצים 700 יחידות.

[5] המידע על הצופן הנאצי במלחמת העולם השנייה הושג בפעילות סוכנות חשאית אמריקאית־בריטית שכונתה TICOM (Target Intelligence Committee). לקראת תום המלחמה הפעילה סוכנות זו צוותים מיוחדים שהצטרפו לכוחות הקדמיים של צבאות בנות הברית ושקדו על איתור סודות הצבא הגרמני, מעצר וחקירה של אנשי צבא גרמנים שעסקו בנושא ואיתור מסמכים וציוד. פעילות זו הייתה חשאית ונשמרה בסוד עד שנת 2009, אז פורסמו לציבור מסמכים רבים. בפעילות זו התברר כי הגרמנים הצליחו לפענח 10 עד 30 אחוזים מהתעבורה שהוצפנה עם M-209, אך בדרך כלל הפענוח נמשך זמן ממושך מדי והיה חסר ערך טקטי. TICOM, *European Axis SIGINT*, Vol. I, 1 May 1946, NSA DOCID 3560861, released 6 January 2009, עמ' 5.
ראו: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/european-axis-sigint/volume_1_synopsis.pdf

מכונת הצפנה אלקטרומכנית
B-211
מנגנון ההצפנה דומה ל־B-21, עם
מקלדת והדפסה על סרט נייר
באדיבות Crypto AG

מכונת הצפנה אלקטרומכנית
M-209
140,000 מכונות מסוג זה יוצרו
עבור צבא ארה״ב במלחמת
העולם השנייה.
המכשיר קטן בממדיו
(178×250×38 מ״מ)
ומשקלו 2.7 ק״ג)
באדיבות Sotheby's

חברת Crypto AG

בתום מלחמת העולם השנייה יזמה שבדיה חקיקה להגבלת מכירות נשק וציוד ביטחוני. בשנת 1948 העתיק בוריס הגלין את פעילותו משבדיה לשוויץ, מדינה ניטרלית שלא הגבילה מכירות נשק, וב־13 במאי 1952 הקים בשוויץ את חברת Crypto AG. הפעילות של החברה השבדית AB Cryptoteknik עברה לחברה החדשה, וכדי לשמור על המוניטין של הגלין שולב השם Hagelin Cryptos בסמליל החברה. בוריס הגלין ניהל את החברה עד פרישתו בשנת 1970. [6]

החברה, עתירת מזומנים בעקבות מלחמת העולם, בנתה במקצועיות ובשיטתיות מעמד של חברה גלובלית מובילה בענף ציוד ההצפנה, תוך התפתחות טכנולוגית רצופה, מרוטורים אלקטרומכניים למעגלים אלקטרוניים, ובהמשך לרכיבי סיליקון מתקדמים ולתוכנה.

[6] Boris Hagelin, *Die Geschichte der "Hagelin Cryptos"*, Crypto AG, 1979

בשנותיה הראשונות החברה התמקדה בפיתוח ובייצור מכשירי הצפנה אלקטרומכניים (מכונת ההצפנה המובילה בשנותיה הראשונות כונתה CX-52),[7] בשנת 1953 החלה לייצר מכונות להצפנת תעבורת טלפרינטרים (המכונה הראשונה כונתה T-52), ובשנת 1966 הקימה מפעל בעיר Zug (מדרום לציריך, כחצי שעה נסיעה), בשלהי שנות ה־60 החלה לייצר ציוד הצפנה אלקטרוני, ובתחילת שנות ה־80 החלה לייצר ציוד הצפנה המבוסס על שימוש בתוכנה. החברה, שהציעה ללקוחותיה ציוד הצפנה מגוון ומתקדם, בחזית הטכנולוגיה, הצליחה למכור ציוד הצפנה לכ־120 מדינות.

בין מוצרי החברה: בשנת 1969 יצא לשוק מכשיר אלקטרוני להצפנת טלפרינטרים בשיטה מקוונת (on-line), T-450, שנרכש בין היתר בידי איראן ומצרים, ובשנת 1970 יצא לשוק מכשיר הצפנה אלקטרוני H-460, מכשיר הצפנה בשיטה לא מקוונת (off line), המכשיר הראשון שעשה שימוש באוגר זיזה (Shift Register) עם משוב לינארי. בשנת 1971 יצא לשוק מכשיר הצפנה לרשתות תג״ם טקטיות CV-096, מבוסס על אפנון דלתא מסתגלת בקצב 9.6 קס״ש, שסופק בין היתר גם לסוריה. בשנת 1972 יצא לשוק מכשיר הצפנה רחב סרט לעורקי רדיו־טלפון טקטיים, MCC-314, בקצב תמסורת של 2.3 מס״ש, שסופק בין היתר לאוסטריה ויוגוסלביה. בתחילת שנות ה־80 יצא לשוק מכשיר הצפנה לרשתות תקשורת נתונים, HC-590, בו מומש אלגוריתם ההצפנה בתוכנה (ולא בחומרה), על מעבד מוטורולה 68000. בתחילת שנות ה־90 יצא לשוק מכשיר הצפנה HC-3300, טלפון מוצפן דיגיטלי עם ווקודר, להפעלה על ערוצי טלפון בקצב של 2,400 סל״ש, ובתחילת שנות ה־2000 יצא לשוק מכשיר ההצפנה HC-2203, גרסה משופרת של המכשיר עם ביצועים טובים יותר, שפעל עד קצב של 19,200 סל״ש, וניהול מרכזי של מפתחות הצפנה. בתחילת שנות ה־2000 יצא לשוק מכשיר הצפנה HC-2423, טלפון סלולרי נייד GSM עם הצפנה מובנית.

סמליל החברה
מחווה לבוריס הגלין

[7] Crypto AG מכרה רישיון לייצור המכשירים לחברה הגרמנית Hell, שייצרה מכשירים אלה עבור צבא גרמניה, בשם H-54.

מפעל Crypto AG ב־Zug, שוויץ, 1976, באדיבות Crypto AG

מכונת הצפנה אלקטרומכנית
CX-52
המכונה יצאה לשוק בשנת 1952, והחליפה גרסאות קודמות, כמו M-209
באדיבות Crypto AG

מכונת הצפנה אלקטרומכנית CX-52 מותקנת על מתאם עם מקלדת, B-52
באדיבות Crypto AG

מכונת ההצפנה האלקטרונית הראשונה T-450
המכונה יצאה לשוק בשנת 1967
באדיבות Crypto AG

מכונת ההצפנה האלקטרונית H-460
המכונה יצאה לשוק בשנת 1970
באדיבות Crypto AG

מערכת הצפנה לדיבור ברשתות רדיו טקטיות בתג״ם CSE-280
מורכבת ממשדר/מקלט SE-035 (יחידה עליונה) ומכשיר הצפנה CV-096 (יחידה תחתונה). יצאה לשוק בשנת 1976.
באדיבות Crypto AG

מכשיר הצפנה לתקשורת רדיו טלפון טקטית MCC-314
בקצב 2.3 מס״ש
באדיבות Crypto AG

המהנדסים והפרופסור

מהנדס שעבד ב־Crypto AG, בשם פטר פרוטיגר (Peter Frutiger), חשד בדבר שיתוף פעולה בין Crypto AG למודיעין הגרמני BND. פרוטיגר ביקר מספר פעמים בדמשק בשנת 1977, כדי לטפל בתלונות על ציוד, וללא הרשאה ממנהליו, ׳תיקן׳ חולשות שמצא. בעקבות זאת התלונן ה־NSA שלא ניתן לקרוא את התעבורה הדיפלומטית של סוריה, ומנכ״ל Crypto AG היינץ ווגנר (Heinz Wagner), שהיה שותף סוד לקשר עם CIA ו־BND, פיטר את המהנדס – למורת רוח ה־CIA, שסבר שיש להמשיך להעסיק את המהנדס ולשמור על ׳שקט׳.

בשנת 1978 גייס ווגנר מהנדסת מבריקה, ד״ר מנגיה קפליש (Mengia Caflisch), שחזרה לשוויץ לאחר מספר שנים בארה״ב. קפליש איתרה ׳חולשות׳ במוצרי Crypto AG, ויחד עם מהנדס נוסף, יורג ספורנדלי (Juerg Spoerndli), איתרו דרך פשוטה ומהירה לפענח את תעבורת מכשיר הצפנת הטלפרינטרים HC-570, אחרי קליטת 100 אותיות בלבד. קפליש המשיכה ׳לעשות בעיות׳, ואחרי מספר שנים תכננה אלגוריתם חדש, בטוח, שמצא את דרכו ל־50 מכונות HC-740 שיוצרו לפני שהמנהלים איתרו זאת. ההנהלה עצרה את יישום השיפור בקו הייצור ו־50 המכונות שכבר יוצרו סופקו לבנקים בשוויץ. התנהגות ההנהלה חיזקה את חשדות המהנדסים בדבר מעורבות חיצונית במוצרי החברה. ה־BND וה־CIA הגיעו למסקנה שהחברה זקוקה לדמות מובילה, שתוכל ׳לרסן׳ את הצוות ההנדסי, ובעזרת סוכנות הביון השבדית איתרו את קייל־אווה ווידמן

(Kjell-Ove Widman), פרופסור למתמטיקה בשטוקהולם ושם בין־לאומי בתחום הקריפטולוגיה, שעבד עם שירותי הביון השבדיים. ווידמן גוייס כ׳יועץ מדעי׳ לחברה, ודיווח ישירות למנכ״ל ווגנר.[8] הידע שלו שכנע את מהנדסי החברה – ואת הלקוחות. ה־BND וה־CIA הקפידו כי חולשות המכשירים לא יתגלו בבדיקות סטטיסטיות מקובלות.

בשנת 1982, כאשר ארגנטינה חשדה שהצופן שלה נפרץ בידי הבריטים במלחמת פוקלנד, ווידמן שכנע אותם שה־NSA שבר ציוד מיושן שעדיין היה בשימושם, אך הציוד החדיש הוא ׳בלתי שביר׳.

הידרה

הידרה (Hydra) הוא שם הקוד של ה־CIA לפרשת האנס בולר (Hans Bühler), נציג מכירות של Crypto AG, שנעצר באיראן באשמת העברת סודות מדינה לשירותי ביון מערביים.[9]

נשיא ארה״ב רונלד ריגן שלח מפציצים אמריקאיים להפציץ יעדים בלוב באפריל 1986, לאחר שהאשים את לוב בפעולת הטרור של פיצוץ מועדון הלילה לה־בל בברלין, בו נהרגו 3 איש ו־229 נפצעו, וציין בדבריו כי השגרירות הלובית במזרח ברלין קיבלה פקודה לבצע את המבצע ודיווחה לטריפולי על הצלחת המבצע. מדבריו היה ברור שארה״ב מפענחת את התעבורה של השגרירות הלובית. איראן, שידעה שלוב משתמשת אף היא בציוד הצפנה תוצרת Crypto AG, החלה לחשוד, ואנשיה קיימו ׳שיחה מתוחה׳ עם האנס בולר (Hans Bühler), איש המכירות של Crypto AG שהיה ממונה על המכירות לאיראן.

שש שנים לאחר מכן, בפברואר 1992, האנס בולר, אז בן 51, שנסע לאיראן בנסיעת עסקים שגרתית להיפגש עם לקוחותיו, נעלם. Crypto AG פנתה לשלטונות שוויץ לסיוע, ואז נמסר להם שהאנס בולר נעצר בידי האיראנים בטענה שהעביר סודות מדינה איראניים לסוכנויות ביון מערביות. נציג קונסולרי שוויצרי ביקר אותו בכלא, ודיווח כי הוא ׳במצב מנטלי קשה׳. תשעה חודשים לאחר מכן שילמה Crypto AG כופר של מיליון דולר (ששולם בידי שירות הביון הגרמני BND. ה־CIA סירב לשלם כופר), והאנס בולר שוחרר וחזר לשוויץ.

האנס בולר לא ידע דבר על הקשר בין Crypto AG ושירותי הביון של ארה״ב וגרמניה, וזועזע מכך שהאיראנים ידעו על החברה יותר ממנו. בהמשך הוא פוטר, תבע את החברה ובין היתר התראיין בשנת 1994 בערוץ טלוויזיה בשוויץ, וטען שבמכשירי ההצפנה שנמכרו לאיראן הייתה ׳דלת אחורית׳ (backdoor) שאיפשרה פענוח התעבורה. החברה הכחישה ותבעה את האנס בולר.[10] הפרשה נגררה שנים בבית משפט, עד שהושתקה.

הפרשה לא נעלמה מעיני לקוחות Crypto AG – ארגנטינה עצרה הזמנה גדולה ; איטליה הפסיקה לרכוש ציוד מהחברה ; ערב הסעודית, הלקוח הגדול של החברה, עצרה הזמנות לבירור העניין ; איש המכירות באינדונזיה העלה חשדות, ומצרים העלתה שאלות רבות. לעומת זאת, איראן המשיכה לרכוש ציוד כמעט מיד.

אירוע האנס בולר היה אירוע הביטחון המהותי במהלך שנות הפעילות, אך לא עצר אותה. עם זאת – אירוע האנס בולר היה ׳הקש ששבר את גב הגמל׳, והביא לפרישת שירות הביון הגרמני מהחברה בספטמבר 1993.

---

[8] פרופסור וידמן עבד בחברה עד שנת 1994, עת חזר לשבדיה לנהל מכון מחקר אקדמי.

[9] *Iran arrests Swiss man for 'espionage'*, UPI, 30 March 1992

[10] הקלטת תוכנית (באנגלית) ברדיו השוויצרי על אירוע ׳הידרה׳ וראיון עם האנס בולר, 2009 (34 דקות): https://www.prosefights2.org/irp2014/p051315/swissradio.mp3

חשיפת פרשת Crypto AG

הפרשה, קריאת התעבורה המוצפנת של מדינות ידידות ויריבות במשך עשרות שנים בידי ה־NSA וה־BND באמצעות שתילת 'חולשות' בציוד ההצפנה שנמכר בידי Crypto AG, נחשפה לראשונה בעיתון בלטימור סאן ב־10 בדצמבר 1995, במסגרת סדרת כתבות על ה־NSA. כתבי העיתון טענו שבמשך שנים ה־NSA הכניס בחשאי חולשות לציוד ההצפנה של Crypto AG, כדי להאזין לתעבורה העוברת בהם, ראיינו את מיודענו יורג ספורנדלי (ראו לעיל) ושמעו את חששותיו, ואספו מעובדים לשעבר בחברה עדויות על כך שבכירה מה־NSA בשם נורה מקבי (Nora L. Mackebee), השתתפה ב'סקר תכנון' למכשירי הצפנה חדשים ב־Crypto AG.[11] כתבי העיתון ראיינו עובדים אחרים ב Crypto AG, שטענו שההאשמות מגוחכות וחסרות בסיס, והנהלת Crypto AG הכחישה האשמות אלה. הפרסום הביא לכך שלקוחות בודדים הפסיקו לרכוש ציוד הצפנה מ־Crypto AG. יתר הלקוחות לא התעניינו במיוחד בכתבות עיתון מבלטימור...

הפרשה נחשפה שוב בפברואר 2020 בידי העיתון וושינגטון פוסט, ערוץ הטלוויזיה הציבורי הגרמני ZDF וערוץ הטלוויזיה השוויצרי SRF. [12] הפרסום, שנשען על מסמך חסוי של ה־CIA שהגיע לידי העיתונאים, חשף את ההיסטוריה של הקשר בין בוריס הגלין ו־Crypto AG ל־NSA, ל־CIA ול־BND.

החשיפות העלו פרטים על הפרשה, כמתואר להלן.

בתחילת 'המלחמה הקרה', בשנות ה־50, סוכנויות הביון בארה"ב התקשו להשיג מודיעין איכותי ולחדור לתקשורת של מדינות יריבות. זו הייתה 'תקופה חשוכה' של הביון האמריקאי, והגורם המרכזי למינוי ועדת בראונל (Brownell Committee) בידי הנשיא טרומן, והקמת הסוכנות לביטחון לאומי בארה"ב NSA, בשנת 1952. [13] החשש מ'עלטה מודיעינית' והצורך של ה־NSA להגיע במהירות להישגים משמעותיים היו בין הגורמים העיקריים ל'מבצע ההשפעה' על Crypto AG, שהפך בהמשך למבצע השתלטות על החברה, מבצע ששירת את שני הצדדים: האמריקאים זכו במודיעין, הגלין נהנה מתשלומים ישירים וסיוע במכירות מוצריו.

משנת 1935 היה בוריס הגלין בקשר עם הגורמים בארה"ב שעסקו בהצפנה. הקשר התהדק והפך לידידות בין הגלין לפרידמן בשנת 1937, והמאמץ של הגלין לסייע לארה"ב בייצור מכשירי הצפנה M-209 במלחמת העולם הידק את הקשר. [14]

בשנת 1954 נרקמה ביוזמת ויליאם פרידמן הסכמה 'ג'נטלמנית' בע"פ בין בוריס הגלין לסוכנות לביטחון לאומי בארה"ב NSA, לפיה בוריס הגלין ימכור רק ציוד שה־NSA יודע לפענח, ולא ימכור ציוד הצפנה

---

[11] Scott Shane, Tom Bowman, *RIGGING THE GAME Spy sting: Few at the Swiss factory knew the mysterious visitors were pulling off a stunning intelligence coup – perhaps the most audacious in the National Security Agency's long war on foreign codes; NO SUCH AGENCY*, The Baltimore Sun, 10 December 1995
ראו:
https://www.baltimoresun.com/1995/12/10/rigging-the-game-spy-sting-few-at-the-swiss-factory-knew-the-mysterious-visitors-were-pulling-off-a-stunning-intelligence-coup-perhaps-the-most-audacious-in-the-national-security-agencys-long-war-on-f/

[12] Greg Miller, *'The intelligence coup of the century': for decades, the CIA read the encrypted communications of allies and adversaries*, the Washington Post, 11 February 2020
ראו: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

[13] Thomas L. Burns, *The Origins of the National Security Agency 1940-1953*, United States Cryptological History, Series V, Volume 1, Center for Cryptologic History, NSA, 1990, NSA DOCID: 3109065, released 2 March 2007
ראו: https://www.govinfo.gov/content/pkg/GOVPUB-D-PURL-gpo73503/pdf/GOVPUB-D-PURL-gpo73503.pdf

[14] *Draft of Historical Record for Boris Hagelin*, NSA REF ID: A61628, released 13 November 2014
ראו:
https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/reports-research/FOLDER_110/42030699106951.pdf

למדינות מסוימות. משפחת הגלין עברה לארה״ב. בהמשך הורחבה הסכמה זו, ונתנה לסוכנויות האמריקאיות זכות סירוב ראשונה לרכישת החברה עם פרישתו של בוריס הגלין.

סיכום ביקור של ווילאם פרידמן ב־Crypto AG בפברואר 1955 חושף את עומק ההסכמות בין ווילאם פרידמן לבוריס הגלין באותה עת, ובין היתר: במכונות ההצפנה החדשות (C-52, CX-52) הוכנסו 'חולשות' שסוכמו בין פרידמן להגלין, Crypto AG הסכימה לא למכור מכשירי הצפנה המבוססים על מפתח חד־פעמי (OTT – One Time Tape), פרידמן הבטיח לתמוך באישור הכנסת המכונות לשימוש נאט״ו ובפעולה לקידום חקיקה גרמנית שתמנע מהתעשייה הגרמנית לייצא ציוד הצפנה.[15] בין היתר כלל הסיכום דיון במכירת ציוד הצפנה למצרים, ירדן (במימון בריטניה), איראן, עיראק, סוריה, ערב הסעודית.

סיכום ביקור נוסף של ווילאם פרידמן ב־Crypto AG בדצמבר 1957, אחרי שיצא לגמלאות (בשנת 1956), חושף את הקשר האינטימי בין ווילאם פרידמן, בוריס הגלין ובכירי Crypto AG, ובין היתר מתאר ביקור במפעל ב־Zug ודיונים במדידות 'קרינת' שדה אלקטרומגנטי מציוד הצפנה, שנעשו בחברת סימנס בגרמניה;[16] בפיתוח מכשירי הצפנה לטלפרינטרים (מעבר מהצפנה לא מקוונת להצפנה מקוונת); ובדגמים השונים של מכשירי ההצפנה T-55 ו־CD-55 (הסיכום מתאר שלושה 'דגמים', הנבדלים זה מזה ב'חוזק ההצפנה': דגם למדינות נאט״ו, דגם למדינות ידידותיות ודגם למדינות אחרות). בוריס הגלין הציג לפרידמן את 'ההסכם הג'נטלמני' בינו לסוכנות הביון הצרפתית ומחשבות למיזוג בין Crypto AG לבין חברת סימנס בגרמניה, ואף דן עמו בקשיים בקשר האישי בינו לבין בנו בו (Bo).[17]

בשנת 1960 נחתם הסכם (Licensing Agreement) בין ה־CIA לבוריס הגלין, והחל מבצע ספרטן (Spartan). ההסכם קבע כי Crypto AG תמכור ציוד הצפנה רק למדינות נאט״ו, לשוויץ ולשבדיה. בוריס הגלין יקבל תמלוגים של 0.6 מ' דולר עבור 'מכירות אבודות' ותשלום שנתי של 75 אלף דולר בגין 'ייעוץ'. מכירות החברה 'זינקו', ממאות לאלפי מכשירי הצפנה בשנה.

בהסכמה עם ה־NSA, Crypto AG מכרה למדינות בדרום אמריקה מכונות הצפנה שה־NSA ידע לפענח.

בשנת 1970 פרש בוריס הגלין מניהול פעיל של Crypto AG והחל מבצע תזאורוס (Thesaurus): שירות הביון הגרמני BND וסוכנות הביון המרכזית של ארה״ב CIA רכשו את השליטה ב־Crypto AG תמורת 25 מיליון פרנק שוויצרי (הרכישה זורזה לאחר ששירות הביון הצרפתי העלה הצעה דומה).

Crypto AG החלה אז לייצר מכשירי הצפנה אלקטרוניים, וה־NSA שלט במודלים הקריפטולוגיים של מכשירים אלה. Crypto AG מיצבה את מעמדה כחברה מובילה בתחום ציוד ההצפנה, ומכירות החברה גאו.

בשנת 1982 חלה בוריס הגלין, אז בן 90, ואושפז לזמן ממושך. מחשש כי ארכיונו האישי יגיע לידיים בלתי רצויות, איש CIA, במסווה של היסטוריון העובד עבור בוריס הגלין, עבר במשרדו של הגלין במפעל ב־Zug על

---

15 *Report of Visit to Crypto AG (Hagelin)*, William F. Friedman, Special Assistant to the Director, NSA 21-28 February 1955, NSA Archive ID: 2436259, released on 22 July 2014
ראו:
https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/correspondence/FOLDER_117/41772899081198.pdf

16 נושא זה, המכונה Tempest, היה מוכר לאמריקאים משנת 1943, ומבוסס היטב כבר משנת 1955. נראה שפרידמן לא חלק מידע זה עם מארחיו. David G. Boak, *A History of U.S. Communications Security*, Volume I, NSA, July 1973, declassified 14 October 2015, עמ' 92. ראו: https://www.archives.gov/files/declassification/iscap/pdf/2009-049-doc1.pdf

17 *Hagelin Negotiations*, Memorandum for the Record, William F. Friedman, 10 January 1958, NSA Archive ID: A60669, released 24 July 2014
ראו: https://nsarchive.gwu.edu/sites/default/files/documents/6779397/National-Security-Archive-20-Draft-of-William.pdf
בו הגלין, שהיה אזרח ארה״ב וחי בארה״ב, נהרג בתאונת דרכים בארה״ב בנובמבר 1970. הוא לא היה שותף סוד לספרטן ותזאורוס.

הארכיון, וסילק ממנו כל מסמך מחשיד. מסמכים אלה הועברו לארכיון ה־CIA. בוריס הגלין לא חזר לעבודה בחברה, ונפטר ב־7 בספטמבר 1983.

בשנת 1987 שונה שם הקוד למבצע מתזאורוס לרוביקון (Rubicon). Crypto AG כונתה מינרבה (Minerva). חברת סימנס הגרמנית כונתה אולימפיה (Olympia) וחברת מוטורולה כונתה נאוואחו (Navaho).

בשנות ה־90 החלה ירידה במכירות Crypto AG, וה־CIA וה־BND נדרשו להזרים לה כספים. הדבר הכביד מאוד על ה־BND.

אחרי איחוד גרמניה באוקטובר 1990 השתנו העדיפויות של ממשלת גרמניה, ומכירת ציוד הצפנה עם 'חולשות' למדינות ידידות לא הייתה מקובלת עליה. העלות הגבוהה של המבצע הכבידה על הגרמנים, ופרשת האנס בולר (ראה לעיל) הגדילה את החשש לחשיפה שתפגע במערכת היחסים הבין־לאומיים של גרמניה. בשנת 1993 פרש שירות הביון הגרמני BND מהפעילות, וה־CIA הופך לבעל השליטה בחברה.[18]

מבט על רשימת הלקוחות של Crypto AG בשנותיה האחרונות נותן תמונה על היקף הכיסוי הגלובלי של גופי הביון של ארה״ב, במדינות יריבות ובמדינות ידידותיות.

THE AMERICAS	EUROPE	AFRICA	MIDDLE EAST	REST OF ASIA
Argentina	Austria	Algeria	Iran	Bangladesh
Brazil	Czechoslovakia	Angola	Iraq	Burma
Chile	Greece	Egypt	Jordan	India
Colombia	Hungary	Gabon	Kuwait	Indonesia
Honduras	Ireland	Ghana	Lebanon	Japan
Mexico	Italy	Guinea	Oman	Malaysia
Nicaragua	Portugal	Ivory Coast	Qatar	Pakistan
Peru	Romania	Libya	Saudi Arabia	Philippines
Uruguay	Spain	Mauritius	Syria	South Korea
Venezuela	Turkey	Morocco	U.A.E.	Thailand
	Vatican City	Nigeria		Vietnam
	Yugoslavia	Rep. of the Congo		
		South Africa		
		Sudan		
		Tanzania		
WORLDWIDE ORGANIZATION		Tunisia		
United Nations		Zaire		
		Zimbabwe		

הפרסום בוושינגטון פוסט, פברואר 2020 – רשימה של 62 מדינות שרכשו ציוד הצפנה מ־Crypto AG

עם השנים, השינויים הטכנולוגיים בעולם התקשורת והמחשבים שינו את אופי השימוש במכשירי הצפנה. העולם עבר להשתמש ביישומי תוכנה במקום מכשירי הצפנה; יעדי גורמי המודיעין ועדיפויותיהם השתנו;

[18] ערוץ הטלוויזיה הגרמני ZDF, בסרט הדוקומנטרי "Geheimoperation 'Rubikon'. Der größte Coup des BND" ששודר ב־18 במרץ 2020, טען שה־BND השתמש במידע שיורט ופוענח משימוש של 'יעדים מודיעיניים' בציוד הצפנה עם 'חולשות' שיוצר ב־Crypto AG עד שנת 2001.

התועלת של המשך המבצע לא עמדה במבחן ההשקעות הכספיות והסיכון המבצעי. חשיפת מסמכי אדוארד סנודן בשנת 2013 העצימה את הסיכון. המבצע הפך לפחות רלוונטי. התקופה של Crypto AG הסתיימה.

חברת Crypto AG נסגרה בשנת 2019, בעסקה שמחקה את עקבות ה־CIA, והתפצלה לשתי חברות, CyOne ו־Crypto International AG, שרכשו את קו המוצרים וחלק מאנשי Crypto AG עברו אליהן.

החקירה הפרלמנטרית בשוויץ

ועדת משנה של ועדת הביטחון בפרלמנט השוויצרי חקרה את הפרשה ופרסמה דו״ח בן 64 עמודים בנובמבר 2020.[19] לצורך הכנת הדו״ח הועבר לעיונה דו״ח מקיף של ה־CIA, בן 100 עמודים, בשם 'MINERVA – A History', שתיאר את מעורבות ה־CIA ב־Crypto AG משנות ה־50. דו״ח זה חסוי ואסור בפרסום.

הוועדה טענה ששירותי הביון בשוויץ ידעו על מעורבות ה־CIA בחברה משנת 1993 והייתה להם גישה למידע שהושג באמצעות פעילות זו, שהיה להם לעזר רב, אך הם לא דיווחו על כך לוועדה, ואף לא סייעו לחקירות המשטרה הפדרלית בפרשת האנס בולר בשנים 1994 – 1995, חקירות שהסתיימו במסקנה כי אין בסיס לחשדות כנגד החברה.

הוועדה מצאה עוד ששירות הביון הפדרלי בשוויץ (NDB (Nachrichtendienst des Bundes השמיד את מסמכי הארכיון שנגעו לקשריו עם ארגוני ביון זרים, על פי סמכותו בחוק, כדי להגן על מקורות.

הוועדה קבעה כי פעולת שירות ביון זר במסווה של חברה שוויצרית היא עבירה פלילית ופוגעת בתדמית שוויץ כמדינה ניטרלית, ולכן הורתה לפעול לביטול רישיונות הייצוא של החברה ולהגשת תביעה פלילית כנגד החברה.

הוועדה מצאה כי Crypto AG לא סיפקה ציוד הצפנה 'חלש' לשימוש שלטונות שוויץ וגורמים פרטיים בשוויץ, אך חברה שוויצרית אחרת, Omnisec AG, שהוקמה בשנת 1987 ונסגרה בשנת 2018, עשתה כן.

סיכום ותובנות

המבצע, בשמות הקוד ספרטן, תזאורוס ורוביקון, היה אחד ממבצעי הביון המוצלחים של המאה. עשרות רבות של מדינות, ידידותיות ויריבות, השתמשו בציוד ההצפנה שנרכש מ'מינרבה', חברת Crypto AG, ה'חולשות' בציוד ההצפנה איפשרו את יירוט המידע ופענוחו, וזה היה אחד ממקורות המידע החשובים של הגרמנים והאמריקאים בתקופת המלחמה הקרה ואחריה. המבצע המחיש את החשיבות המודיעינית של האזנה לתקשורת, והעניק יתרונות חשובים לארה״ב ולגרמניה.

[19] *Fall Crypto AG Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte vom 2*, Geschäftsprüfungskommissionen , 10 November 2020
ראו: https://www.parlament.ch/centers/documents/de/bericht-gpdel-2020-11-10-d.pdf

לפי הפרסום בוושינגטון פוסט מפברואר 2020, דו"ח ה־CIA מסכם: "זה היה מבצע המודיעין של המאה. ממשלות זרות שילמו סכומים טובים לארה"ב ולגרמניה המערבית עבור הזכות לקרוא את התקשורת הסודית ביותר שלהן לפחות על ידי שתי (ואולי עד חמש או שש) מדינות זרות".[20]

עלילות Crypto AG ממחישות את חשיבות היכולות הטכנולוגיות העצמיות של מדינה לביטחונה הלאומי, ואת היכולת של מעצמות טכנולוגיות לפגוע בביטחון לאומי של מדינות אחרות.

מפעל Crypto AG ב־Steinhausen, שוויץ, 2017 לערך
באדיבות Crypto AG

[20] הכוונה כנראה למדינות השותפות באמנת Maximator משנת 1976, בדבר שיתוף פעולה מודיעיני בין ארה"ב, גרמניה, דנמרק, הולנד, צרפת ושבדיה.

ציר הזמן

תיאור כרונולוגי של 'עלילות' בוריס הגלין ו־Crypto AG מציג תמונה מקיפה של האירועים:

שנה	אירוע
1892	בוריס הגלין (Boris Casear Wilhelm Hagelin) נולד באזרבייג'ן, לתעשיין שבדי שניהל את שדות הנפט ליד באקו עבור משפחת נובל.
1914	בוריס הגלין סיים לימודי הנדסת מכונות באוניברסיטה הטכנית בשטוקהולם.
1915	קצין צי שבדי, Olof Gyldén, ומהנדס שבדי Arvid Gerhard Damm, ייסדו בשבדיה חברה לפיתוח וייצור ציוד הצפנה, בשם AB Cryptograph.
1921	משפחת נובל ומשפחת הגלין (Karl Wilhelm Hagelin, אביו של בוריס הגלין) נכנסו כשותפים ל־AB Cryptograph.
1922	בוריס הגלין הצטרף ל־AB Cryptograph, כמנהל הכספים.
1925	בוריס הגלין מונה למנהל הכללי של חברת AB Cryptograph.
1932	הוקמה חברת AB Cryptoteknik, בבעלותו של בוריס הגלין, ונכסי חברת AB Cryptograph עברו אליה.
1937	AB Cryptoteknik מוכרת לצבא ארה"ב את זכויות הייצור של מכונת ההצפנה C-38 תמורת 8.6 מ' דולר. המכונה יוצרה בארה"ב בשם M-209 ויוצרו ממנה 140,000 יחידות. זו הייתה מכונת ההצפנה לדרגי השדה בצבא ארה"ב במלחמת העולם השנייה.
1948	בוריס הגלין עובר לשוויץ.
1952	בוריס הגלין מקים בשוויץ את חברת Crypto AG, ומעתיק אליה את פעילות AB Cryptoteknik. Crypto A הקימה מפעל בעיר Zug. שוויץ, כמדינה ניטרלית, יכלה לסחור עם כל מדינות העולם ללא מגבלות.
1954	הסכמה 'ג'נטלמנית' בע"פ בין בוריס הגלין לסוכנות לביטחון לאומי בארה"ב NSA, לפיה בוריס הגלין ימכור רק ציוד שה־NSA יודע לפענח, ולא ימכור ציוד הצפנה למדינות מסוימות. משפחת הגלין עברה לארה"ב. ה'הסכמה הג'נטלמנית' נתנה לסוכנויות האמריקאיות זכות סירוב ראשונה לרכישת החברה עם פרישתו של בוריס הגלין.
1957	Crypto AG מכרה בחשאי מכשירי הצפנה CX-52 למדינות 'אסורות': בורמה, עיראק, אינדונזיה, איראן, ירדן, יוגוסלביה, לבנון, מרוקו ותוניסיה.
1958	הפסקת פעילות הייצור ב־AB Cryptoteknik בשוודיה.
1960	מבצע ספרטן (Spartan): נחתם הסכם בין בוריס הגלין ל־CIA. Crypto AG תמכור ציוד הצפנה רק למדינות נאט"ו, לשוויץ ולשבדיה. בוריס הגלין יקבל תמלוגים של 0.6 מ' דולר עבור 'מכירות אבודות' ותשלום שנתי של 75 אלף דולר בגין 'ייעוץ'. מכירות החברה 'זינקו', ממאות לאלפי מכשירי הצפנה בשנה. בהסכמה עם ה־NSA, Crypto AG מכרה מכונות הצפנה שה־NSA ידע לפענח למדינות בדרום אמריקה.
1965	Crypto AG הוציאה לשוק מכונת הצפנה אלקטרונית ראשונה, CX-52M, שעשתה שימוש באוגר זיזה (Shift Register) עם משוב לינארי, שמומש באמצעות טרנזיסטורים. ה־NSA שלט במודל הקריפטולוגי של מכשיר זה.
1966	Crypto AG הקימה מפעל נוסף בעיר Steinhausen, כעשר דקות נסיעה מהמפעל ב־Zug.
1970	בוריס הגלין פורש מניהול Crypto AG. מבצע תזאורוס (Thesaurus): שירות הביון הגרמני BND וסוכנות הביון המרכזית של ארה"ב CIA רוכשים את השליטה ב־Crypto AG תמורת 25 מיליון פרנק שוויצרי. הרכישה נעשתה לאחר ששירות הביון הצרפתי העלה הצעה דומה. Crypto AG הוציאה לשוק מכונת הצפנה אלקטרונית, H-460, והפסיקה ייצור מכונות הצפנה אלקטרומכניות.
1982	בוריס הגלין, בן 90, אושפז לזמן ממושך. מחשש כי ארכיונו האישי יגיע לידיים בלתי רצויות, איש CIA, במסווה של היסטוריון העובד עבור בוריס הגלין, עבר על הארכיון וסילק ממנו כל מסמך מחשיד. מסמכים אלה הועברו לארכיון ה־CIA.
1983	בוריס הגלין נפטר.
1987	שם הקוד למבצע שונה מתזאורוס לרוביקון (Rubicon). Crypto AG כונתה מינרבה (Minerva). חברת סימנס הגרמנית כונתה אולימפיה (Olympia) וחברת מוטורולה כונתה נאוואחו (Navaho).
1992	פרשת הידרה (Hydra) – האנס בולר (Hans Bühler), נציג מכירות של Crypto AG, נעצר באיראן, שוחרר לאחר תשעה חודשים לאחר שהחברה שילמה כופר של מיליון דולר, פוטר

שנה	אירוע
	מהחברה, תבע את החברה, ובין היתר טען שבמכשירי ההצפנה שנמכרו לאיראן הייתה 'דלת אחורית' (backdoor) שאיפשרה את פענוח התעבורה. החברה הכחישה ותבעה את האנס בולר. הפרשה נגררה שנים בבית משפט, עד שהושתקה. זו הייתה אחת הסיבות ששירות הביון הגרמני פרש מהחברה.
1993	שירות הביון הגרמני פורש, מחשש לחשיפה, וה־CIA הופך לבעל השליטה בחברה.
1995	עיתונאי בבלטימור סאן פרסם בדצמבר 1955 מאמר על פרשת האנס בולר. Cryto AG הכחישה, והעניין בנושא דעך.
2009	הרדיו השוויצרי שידר תוכנית על האירוע וראיון עם האנס בולר.
2014	ה־NSA שחרר 7,600 מסמכים (52,000 דפים) הקשורים לוויליאם פרידמן, מהשנים 1939 עד 1969. 400 מהמסמכים מתייחסים לבוריס הגלין ו/או־Crypto AG, ומהם מתבררת ההסכמה ה'ג'נטלמנית' של שנת 1954.
2018	האנס בולר נפטר.
2019	חברת Crypto AG נסגרה, בעיסקה שמחקה את עקבות ה־CIA. החברות CyOne ו־Crypto International AG רכשו את קו המוצרים וחלק מאנשי Crypto AG עברו אליהן.
2020	מבצע רוביקון נחשף בידי העיתון וושינגטון פוסט, ערוץ הטלוויזיה הציבורי הגרמני ZDF וערוץ הטלוויזיה השוויצרי SRF.
עד היום	חברת CyOne מוכרת ציוד הצפנה לממשל השוויצרי. חברת Crypto International AG מוכרת בעולם סדרה של מכשירי הצפנה. החברה מציגה את עצמה כאחת החברות הוותיקות והמכובדות בעולם בתחום מכשירי הצפנה, ומבטיחה ללקוחותיה מוצרים מוכחים, להתמודדות נאותה מול איומי האזנה למידע.

הערה בעניין מקורות

מסמך ה־CIA, 'MINERVA – A History' טרם נחשף. הפרסום בוושינגטון פוסט (לעיל, הערה 12) הציג קטעים ממנו, המוצגים בנספח.

תיק התכתבויות בין פרידמן והגלין בשנים 1943 עד 1969 נחשף ביד ה־NSA, וזמין בתיק ACC47111 באוסף מסמכי ווילאם פרידמן באתר ה־NSA.

באתר ההולנדי Crypto Museum מידע על המוצרים ופרסומים רבים של חברת Crypto AG.[21]

אתר האינטרנט של Crypto AG זמין בארכיון האינטרנט (https://archive.org/). לדוגמה:

- 24 במאי 1998: https://web.archive.org/web/19980524180249/http://www.crypto.ch/
- 30 במאי 2002: https://web.archive.org/web/20020530170046/http://www.crypto.ch/
- 4 במאי 2012: https://web.archive.org/web/20120504105630/http://www.crypto.ch/
- 4 במאי 2016: https://web.archive.org/web/20160504060004/http://www.crypto.ch/

נספח

הנספח כולל קטעים שפורסמו בוושינגטון פוסט מתוך מסמך ה־CIA – 'MINERVA – A History'.

[21] ראו: https://www.cryptomuseum.com/crypto/hagelin/index.htm

נספח: קטעים שפורסמו מתוך מסמך ה־CIA – 'MINERVA – A History' [22]

המהנדסים והפרופסור

מנגיה קפליש חכמה מדי:[23]

(S) Early the following year Wagner hired a bright new engineer, Dr. Mengia Caflisch -- again, without consulting the Partners. NSA quickly realized that she was too bright to remain unwitting, and frantically tried to cancel the hiring. Wagner was unmoved, and Caflisch stayed. But NSA had been right. She was too bright, and soon broke the new 500 cryptology through a known plain text attack. She went on to expose the cryptographic weaknesses of other CAG products, and proceeded to design her own, unbreakable, cryptologics. Her technical brilliance attracted a following among several CAG engineers.

קייל־אווה ווידמן (הנרי) כונה בשם הקוד אתנה:

(S) Unable to pronounce his name, his American friends called him Henry. Widman carried this name with him for the rest of his life, and was known informally to MINERVA teammates as Henry. His cryptonym became ATHENA, the goddess of wisdom (and war).

פרופ׳ ווידמן (הנרי) ראה בעבודתו שליחות למען העולם החופשי:

(S) Rick Schroeder was then introduced in his true CIA colors, and they talked awhile longer. Henry said he was willing, and they shook hands. When they entered the garden where the luncheon was in progress, it was thumbs up. There was much congratulating and Gemutlichkeit. The luncheon became an event.

(S) Years later, Henry recalled the lunch. He felt that he had been welcomed into a secret society, and had learned the secret handshake. These people had become colleagues engaged in a critical struggle for the benefit of Western intelligence. These were people he could work with. It was, he said, the moment in which he felt at home. This was his mission in life.

ה׳בלוף׳ (של ווידמן, בארגנטינה) פעל...

(S) When faced with customer revolt, he would get on a plane, sometimes alone, sometimes with Wagner, and fly off to confront the customer. This tactic led to several trips to Latin America to calm the waters. Chile continued to complain about weak CAG cryptologics, and Henry was afraid that the Chilean navy was just inches away from breaking its own 503 machine. When the Chileans threatened to buy Datotek equipment, Henry assured them that Datotek could not get an export license. (Since Chuck Kinney was himself the approving authority, Henry was on solid ground.) Instead, Henry assured the suspicious Chileans that he would provide a more secure cryptologic just for them. Chile was thus saved as a CAG customer.

(S) After the Falkland Islands War, the Argentines discovered that the British and Americans had broken their systems. The furious Argentines summoned Henry to Buenos Aires to explain. The matter was not simple, said Henry, but it appeared that NSA had broken an analog speech system -- these systems were notoriously weak, he said, but the CAG 500 systems were unbreakable. The bluff worked. The Argentines swallowed hard, but kept buying CAG equipment.

---

[22] הפרסום נעשה בוושינגטון פוסט ב־11 לפברואר 2020 (לעיל, הערה 12). המדובר כנראה בקטעים מתמצית פרסום של ה־CIA שנכתב בשנת 2004, עליו נרשמו הערות של ה־BND.

Richard J. Aldrich, Oeter F. Müller, Davud Ridd and Erich Schmidt-Eenboom, *Operation Rubicon: Sixty Years of German-American success in signals intelligence*, Intelligence and National Security, 35 (5), 4 June 2020, pp. 603-607. https://wrap.warwick.ac.uk/137156

[23] CAG הוא קיצור ל־Crypto AG.

הידרה

איראן, לקוח חשוב של Crypto AG, הייתה יעד מועדף של ה־NSA:

(TS) The most lucrative target using influenced crypto was Iran. The Iranian target was 80-90 percent readable, thanks to the Iranian penchant for buying from MINERVA. In 1988, over 19,000 Iranian decrypts were turned into product reports, covering everything from hostage issues to the Iranian conflicts with other Gulf States.

האזנה לאיראנים הייתה חשובה בשיחות לשחרור החטופים האמריקאיים בשנת 1980:

(TS) The negotiations to repatriate the American hostages in Iran dominated the late Carter years. To President Carter, it was critical to know what the Iranians were up to, and since the Algerians were acting as intermediaries, that information came from Algerian diplomatic communications. Admiral Bobby Inman, then DIRNSA, recalled in an interview that the President would frequently call him at his office at Fort Meade to request information that NSA could gain through Algerian communications. Those communications, Inman said, were MINERVA-enabled, and this was the "absolutely critical ingredient" in enabling the President to appreciate the situation and manage the negotiations.

שירות הביון הגרמני BND החליט לשלם לאיראנים כופר של מיליון דולר לשחרור האנס בולר:

(S) The next day Munich was informed that the White House had rejected the "bail" sophistry. It was clearly "ransom," and could not be paid. BND President Konrad Porzner was to be informed that no American money was to be used to secure Buehler's release.

(S) When informed of the American stance, Porzner decided that if necessary Germany would proceed alone, and pay the entire $1 million. Perhaps the Americans could be talked into paying their share later, but even if they could not, this was too important a matter to let a peculiarly American prohibition stop the release of Buehler. Germany was under no such prohibition, and would do what it believed was necessary.

Michael Grupe, מנכ"ל Crypto AG, הכחיש בצורה משכנעת את ההאשמות של האנס בולר:

(S) Grupe appeared on camera, interviewed by a Swiss journalist. He bluntly denied the allegations, terming them warmed-over claims by disgruntled employees. Buehler was fired because company management had lost trust, and because he refused to turn over his lawyer's files to the firm. He dismissed as "insanity" the allegations that the Germans were manipulating the gear. CAG sold in Germany, he pointed out, and in Switzerland, which had given the company a "clean bill of health." The whole thing was utter nonsense. As to allegations that foreign intelligence organizations were known to visit CAG, of course they had. They were customers, and good ones. They trusted the security of CAG gear.

(S) Grupe's appearance cast enough doubt on Buehler's allegations to blur the issue. Langley hoped that viewers would come away at least a little confused about charges that had seemed so clear in pre-program and pre-book publicity. Grupe's performance was credible, and may have saved the program.

תגובת הלקוחות לפרשת האנס בולר:

(S) For customers, the Buehler affair came as a shock. The Argentine Navy threatened to buy everything from other suppliers, and a government decision to make a major purchase from CAG was immediately placed under review. The Italians, always a little skittish about CAG products, seemed likely to fly out of the CAG orbit. The Saudis, the single biggest customers, halted orders pending clarification. The CAG salesman in Indonesia was having trouble defending CAG products, and appeared to have his own suspicions. Egypt began peppering the company with questions about crypto security. One of the few countries that showed little reservation was Iran. It resumed its purchase of CAG equipment almost immediately.

נמלטנו בעור שיננו:

(S) The HYDRA affair was the most serious security breach in the history of the program, and its aftershocks continued to rumble through the end of the decade. But it did not cause its demise, and at the turn of the century MINERVA was still alive and well. It was a very narrow escape.

חשיפת פרשת Crypto AG

בשנות ה־50, שיפורים בהצפנה של יריבים גרמה 'לתקופה החשוכה' של מנתחי הצפנים בארה"ב:

(S) When, in 1950, North Korean forces attacked the south, Army codebreakers cracked the North's communications security like a nut in a vise. A year later that effort, too, was in tatters, a victim of North Korean communications security improvements. The codebreakers were to read none of the enemy's high-level systems for the rest of the war.

(S) And so American codebreaking entered into a period that CIA official Charles Collins once called "the Dark Ages of American cryptology." When Dwight Eisenhower became president, American cryptologists were reading none of the high-level ciphers of their three principal enemies.

בשנת 1951 החלה להירקם עסקה סודית בין ויליאם פרידמן ובוריס הגלין:

(S) When Hagelin arrived in Washington, he and Friedman went to dinner at Friedman's favorite haunt, the exclusive Cosmos Club. Over dinner, Friedman set forth quite a different menu. Would it be possible, Friedman asked, to control the sale of the new machines in such a way that only certain countries could purchase the newer, more secure, machines? Hagelin sounded interested, and agreed to hear what Friedman's organization, the Armed Forces Security Agency (AFSA), had to offer.

ההסכם של שנת 1960 מיסד בכתב את ההסכמה ה'ג'נטלמנית':

(S) The Licensing Agreement was not much different, technically, from the Gentlemen's Agreement, but it was in writing. Hagelin could sell any machine to any NATO countries, plus Switzerland and Sweden. As for the rest, the agreement had an attached chart showing who could buy what. It was to last for five years, with automatic renewals annually past 1965 for another ten years. After 1975, renewals would require specific concurrence from both parties. The United States would have patent rights to all Hagelin equipment (except for the pocket device, which Bo still possessed) for the duration of the agreement.

ה־CIA וה־BND הגיעו להסכמות ביוני 1970:

(S) The sale was made on 4 June, and the agreement with the BND was contained in a 12 June 1970 memorandum of understanding between CIA and the BND. For CIA, COB Munich Tom Lucid signed, in a hand made shaky by Parkinson's disease, while the BND signature was illegible. It specified that the BND, operating through Deutsche Truehand Gesellschaft-Munich (DTG-M), would purchase AEH. The sale price was 25 million Swiss Francs, 8.5 million to be paid at contract closing, and the remainder to be paid in two equal installments on 1 June 1971 and 1 June 1972. Hagelin had remarried in 1969, and insisted that a pension be provided for his new wife -- Elsa Hagelin (nee Svensson), his late wife's former nurse -- after his death. All decisions would be subject to joint CIA-BND concurrence.

מכירות החברה גאו – זה היה העסק הרווחי ביותר 'במלחמה הקרה':

Table 3
(S) Crypto AG: Sales and Profits, 1970-1975

Year	Sales (SFr)	Profits (SFr)	Profit as a Percentage of Sales
1970	15.17	1.38	9%
1971	15.86	.83	5%
1972	19.17	3.47	18%
1973	27.59	2.90	10%
1974	34.48	4.12	12%
1975	51.27	4.41	8.6%

למשתתפים ולחברות ניתנו שמות קוד, ובשלהי שנות ה־80 שם המבצע שונה לרוביקון:

(S) To cover the whole arrangement, CIA and the BND agreed to a special cryptonym series. CAG would always be referred to as MINERVA, so as not to have to use the true company name. Foreign players in the game got cryptonyms. Nyberg, the only original CAG player who was witting, was named BALL, while his technical, but unwitting, counterpart, Oscar Stuerzinger, was called SIEGFRIED.

(S) Each major organization got a cryptonym: thus, CIA was EOS, NSA was HOCKEY, BND was GAMMA, ZfCh was SIGMA, and Siemens was OLYMPIA. The American firm Motorola, which had been brought into the MINERVA equation in the 1960s, was called NAVAHO. AEH, the holding company that owned Crypto AG, was called GOLF. Even DTG, the accounting firm, had a cryptonym. It was called FIDELIO.

(S) The Partners named their joint project THESAURUS. In the late 1980s they changed the name to RUBICON. They held periodic conferences to establish or change policy. Essentially, the conferences undertook the role of a covert board of directors.

בשנות ה־90 קטנו המכירות, ו־BND וה־CIA נדרשו להזרים כספים לחברה:

1. (S) Diverging worldviews resulting from the end of the Cold War, in which Germany was drawing closer to its European partners, and was increasingly reluctant to sell readable gear to European nations. Since the German reunification of 1990, the Germans constantly reminded the Americans of their new status in the world.
2. (S) The increasing need for infusions, which the Germans could ill afford. (Moreover, the involvement of a partner in the infusion mechanism made the process all the more complex and slowed down the arrival of the money into the CAG coffers.)

האמריקאים רצו להאזין לכולם, הגרמנים היססו להאזין למדינות ידידות:

(S) Cipher readability was a vexing question. Why produce readable and unreadable equipment, NSA officers asked themselves, if they could sell readable equipment to everyone? So as time went on, the American position began to change. Americans became less and less agreeable to selling secure equipment to anyone. Why secure Spanish communications if they were yielding useful information? Why, indeed, secure the communications of some of the NATO countries? Greece and Turkey were taken off the "secure" list at a very early date, even though they were NATO partners. The list of protected nations became shorter by the year.

(S) Germany, with a Eurocentric outlook, strongly supported the two-cryptologies approach. The BND did not like to sell readable equipment to its allies. According to bilateral MINERVA agreements, the BND had to concur in all CAG sales. But NSA remained tenacious, and in the long run, only a handful of NATO nations directly or indirectly involved in MINERVA, plus Sweden and Switzerland, remained protected.

סיכום ותובנות

כ־40 אחוז מהתעבורה שה־NSA יירט ופענח וכ־90 אחוז מהתעבורה הדיפלומטית שה־BND יירט ופענח התבססה על יירוט תעבורה שהשתמשה בציוד הצפנה תוצרת Crypto AG:

(TS) The American-German partnership on MINERVA had continued for over twenty years. To the Americans it represented over 40 percent of NSA's total machine decryptions, and was regarded as an irreplaceable resource. To the Germans, however, it was even more important, accounting for 90 percent of the BND's diplomatic product reports. The BND regarded it as the linchpin of its highly productive intelligence relationship with the Americans.

זה היה מיזם המודיעין המהותי של המלחמה הקרה:

(S) German and American case officers who had worked together remember the days of MINERVA with fondness. For almost everyone it was the highlight of their careers. Even during periods of disagreement, there was a recognition that the greater good of Western intelligence required that the project continue to run smoothly. Cultural differences, and the divergent interests of the two countries, were overcome, again and again, to fashion the most profitable intelligence venture of the Cold War.