# הצי השקט: כלי מחקר תת ימיים חשופים לאינטרנט
# AUVs – Autonoumous Underwater Vehicle

מאת אמיתי דן

## הקדמה

מחקר זה חושף כי תשתית פיקוד ושליטה של כלי שיט תת ימיים אוטונומיים הייתה נגישה מהאינטרנט במגוון אוניברסיטאות ומכוני מחקר לאורך תקופה של שנים רבות.

המחקר טוען כי מתודולוגיות של פיתוח מאובטח לא הוטמעו, וארכיטקטורת השליטה והבקרה נבנתה באופן פרוץ .תוקף פוטנציאלי יכל לצפות במיקום הרחפנים, לקרוא את נתוני המחקר, לשלוח להם פקודות, לתת הוראות שיט לפגוע במחשב המדעי של הכלים ולנסות לפרוץ דרך מערכת השליטה והבקרה למכון המחקר/אקדמיה שממנה נשלט הכלי.

## רקע, מתודולוגיה וכלי השיט

**רקע והגדרת הכלי**

דאון תת ימי הוא סוג של רכב תת ימי אוטונומי:

Underwater glider is a type of autonomous underwater vehicle (AUV)

אז מי המציא אותו?

דאגלס ס. וב (Douglas C. Webb) היה מהנדס ואוקיינוגרף חלוצי, מייסד חברת Teledyne Webb Research (לשעבר Webb Research Corp), ומוכר בעיקר בזכות המצאת כלי השיט האוטונומי לחקר האוקיינוסים, ה"סלוקום גליידר" (Slocum Glider)

הנה כמה עובדות מרכזיות על ההמצאה ופועלו:

הרעיון: הגליידר תוכנן לנוע ברחבי האוקיינוסים תוך חיסכון אנרגטי עצום. במקום מנוע מדחף קונבנציונלי, הכלי משתמש בשינויי ציפה (Buoyancy) בשילוב עם כנפיים, המאפשרים לו לנוע אנכית ואופקית בתנועה דמוית מסור דרך עמודת המים.

מקור השם: כלי השיט נקרא על שמו של ג'ושוע סלוקום (Joshua Slocum), האדם הראשון שהקיף את העולם לבדו בסירה.

חלוציות ושימושים: הגליידרים של וב מסוגלים לשהות בים חודשים ארוכים ולחצות אוקיינוסים שלמים. הם משמשים למחקר אקדמי, מעקב אחר יונקים ימיים (כגון לווייתנים), איסוף נתונים על זרמים, טמפרטורה ומליחות, וכן למשימות צבאיות.

לצפיה נוספת: https://vimeo.com/711991309

למה לא איבטחו את כלי המחקר?

מה גורם לפתח ולשלוח ללב ים כלי שיט תת ימיים ללא כל אבטחה? בניגוד לשרת שאפשר לאפס לו סיסמא, מדובר על כלי מחקרי שמתפקד כמו לוויין תת ימי. אם הוא יינעל וילך לאיבוד בגלל שמישהו שכח סיסמא, מחקר אקדמאי של שנים עלול לרדת לטמיון. זה המתח שבין אבטחה לבין תפעול מנקודת המבט של החברה המפתחת, במקרה שבו חוקרים שולחים כלים תת ימיים למסע ארוך בלב ים ולא רוצים לאבד כלי יקר ערך ומחקר שירד לטמיון כי מישהו שכח סיסמא בים.

**תרגום לעברית מתוך מדריך ההפעלה של Slucom Glider**

**"אימות דאון (Glider Authentication)**

דאונים המתחברים לשרת עגינה דרך אירידיום עשויים באופן אופציונלי להידרש לאימות לפני שתורשה להם גישה לשרת העגינה. אלא אם ישנן סיבות מכריעות לדרוש אימות דאון, מומלץ לא להשתמש ביכולת זו.

זה קשה מספיק לתקשר עם דאון בים ללא המחסום הנוסף של רצף התחברות. זה מעלה את ההסתברות שדאון בים יהיה ללא קשר עקב תצורה שגויה, שגיאת תוכנה, קובץ פגום, סיסמה אבודה, וכו'."

התפיסה השניה שמלווה את המחקר ואת הליך הדיווח, היא שאין פה מה לגנוב, זה רק כלי מחקרי תמים ואיטי. הסינים חשבו אחרת בתקרית שבה כלי זהה לכלים שנחשפו במחקר זה, אשר שייך לצי האמריקאי, נאסף על ידי הצי הסיני. במחקר זה לא נחשפו ישירות כלים השייכים לצי האמריקאי, אך חולשות האבטחה שאותרו רלוונטיות לכלל המשתמשים, ככל שישנו שימוש בגרסאות לא מעודכנות.

השימושים המוגדרים של ה-(United States Fleet Forces Command) USFCC בכלים אלו הוא סיוע לתחומי לוחמה מרכזיים ואת השילוב שלהם עם כוחות מיוחדים, לכן להבנתי מדובר על כלי מחקרי דו שימושי שרצוי לשנות את תפיסת הפיתוח והתפעול שלו ושל כלים שדומים לו ומשמשים למחקר ולפעולות צבאיות וביטחוניות. המתיחות הנוכחית מול איראן מסבירה למה התווך התת ימי רלוונטי מתמיד ומה החשיבות של אבטחת כלים אלו לאפשור של ביצוע משימות ימיות.

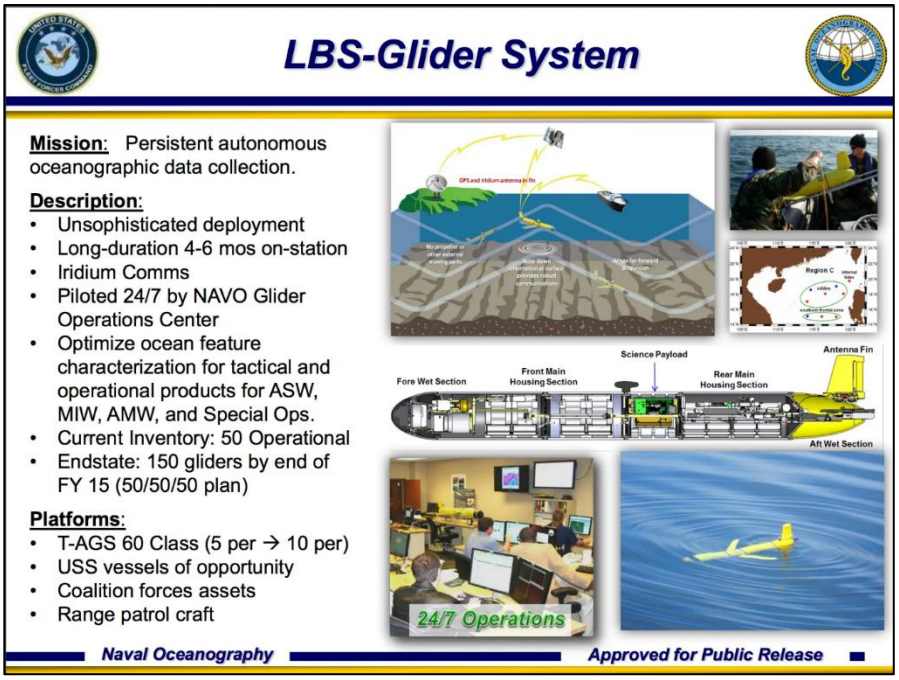
## הגדרות

**AMW (לוחמה אמפיבית – Amphibious Warfare):** תכנון וביצוע של מבצעים המשלבים כוחות ים ויבשה (כמו חיל הנחתים/המרינס). המטרה היא להנחית כוחות, ציוד ולוחמים מהים אל חוף האויב.

**MIW (לוחמת מוקשים – Mine Warfare):** גילוי, זיהוי ונטרול של מוקשים ימיים כדי לאפשר שיט בטוח לספינות ידידותיות, לצד היכולת להניח מוקשים כדי לחסום את האויב.

**ASW (לוחמה נגד צוללות – Anti-Submarine Warfare):** איתור, מעקב והשמדה של צוללות אויב באמצעות שילוב של ספינות טילים, מטוסים, מסוקים, סנסורים מתקדמים ומערכות נשק (כמו טורפדו).

Special Operations (Special Ops) directly intersects with the AMW, MIW, and ASW domains to support elite forces like Navy SEALs and SWCC (Special Warfare Combatant-craft Crewmen).



## Statement by Pentagon Press Secretary Peter Cook on Incident in South China Sea

Dec. 16, 2016 |

Using appropriate government-to-government channels, the Department of Defense has called upon China to immediately return an unmanned underwater vehicle (UUV) that China unlawfully seized on Dec. 15 in the South China Sea while it was being recovered by a U.S. Navy oceanographic survey ship. The USNS Bowditch (T-AGS 62) and the UUV -- an unclassified "ocean glider" system used around the world to gather military oceanographic data such as salinity, water temperature, and sound speed - were conducting routine operations in accordance with international law about 50 nautical miles northwest of Subic Bay, Philippines, when a Chinese Navy PRC DALANG III-Class ship (ASR-510) launched a small boat and retrieved the UUV. Bowditch made contact with the PRC Navy ship via bridge-to-bridge radio to request the return of the UUV. The radio contact was acknowledged by the PRC Navy ship, but the request was ignored. The UUV is a sovereign immune vessel of the United States. We call upon China to return our UUV immediately, and to comply with all of its obligations under international law.

**כלי השייט התת-מימי האוטונומי – Slocum Glider**

כלי השייט התת-מימי האוטונומי (AUV) מסוג Slocum Glider, שנבנה על ידי תאגיד Teledyne Webb Research (מפאלמות', מסצ'וסטס), הוא פלטפורמת מכשור משולבת המיועדת לפעול באזורי חוף באוקיינוסים עד לעומק של 1,000 מטרים. ההנעה העיקרית שלו מתבצעת באמצעות שינויי ציפה המופעלים על ידי מנוע זבורית (ballast) בחזית הכלי. מנגנון זה מאפשר לרובוט בעל הכנפיים לצלול ולעלות בזווית גלישה מוגדרת, וכך להשיג מהירות התקדמות. ההיגוי מתבצע באמצעות הגה כיוון הממוקם בזנב הכלי.

התוצאה היא כלי תת-מימי אוטונומי בעל צריכת אנרגיה נמוכה ויכולת פעולה ממושכת, מה שהופך אותו לבעל יכולת התאמה גבוהה עבור תצפיות באוקיינוס. בזמן הפעלתו בשטח, הרובוט מתקשר ומעלה נתונים דרך קישור לווייני של רשת אירידיום (Iridium), מה שמאפשר קשר עם מפעילים ומדענים ברחבי העולם.

בין אם המשימה היא פרויקט של סטודנט לתואר מתקדם, איסוף נתונים עבור מודלים לחיזוי הוריקנים, או דגימה המשתרעת על פני אוקיינוס שלם, הדאון (glider) הפך לכלי המועדף עבור מיזמים רבים של ניטור אוקיינוסים.

*Unmanned Warrior 2016 Mission Theme: Geospatial Intelligence

# Slocum Gliders

## AT A GLANCE

### WHAT IT IS:

Underwater gliders "fly" in the ocean by changing buoyancy or using a propeller. These UUVs can remain at sea for months at a time, continuously collecting environmental information to better understand how the ocean works.

### HOW IT WORKS:

Traditional gliders propel themselves forward by changing their buoyancy to sink or rise through the water column. "Hybrid" vehicles can make use of a prop ("thruster") to increase forward speed and escape environmentally hazardous areas. While they glide up and down from the ocean surface to depths as great as 1000 meters, they measure the temperature, conductivity, and optical (light) properties of the water they pass through.

### WHY IT IS IMPORTANT:

Data collection from gliders provide near real-time measurements of conditions at a greater data volume and fraction of the cost of traditional platforms. This in turn enhances the ocean model nowcasts and forecasts to yield faster and greater environmental insight to naval operational commanders.

**Unmanned Warrior is part of exercise Joint Warrior 2016, hosted by the United Kingdom off the North-West coast of Scotland.*

Sensors aboard Unmanned Underwater Vehicles (UUV) gather data on the physical properties of the ocean environment in real-time. This information is then transmitted back to a shore-side facility for use in real-time oceanographic models, historical databases, and environmental assessment products.

This data has been used by scientists in the study of temperature effects on the strength of hurricanes and typhoons. It is also used by divers in determining horizontal and vertical visibility. UUVs outfitted with additional sensors are used in environmental studies and gathering meteorological data for weather prediction.

Due to their ability to collect massive amounts of data over long time periods at low cost, UUVs like the Slocum glider are becoming increasingly important to the Navy to better inform the warfighter. Measurements made by gliders are used in the investigation of mine and/or "mine-like" objects to support naval sub-surface security.

Unmanned Warrior 2016, allows the US Navy, the British Royal Navy and allies to test UUVs in real operating environments with coalition forces. Gliders will be deployed from shore-based facilities as well as ships of opportunity, and operate in varying water depths off the North-West Scottish coast line.

**Research Objectives for US in Unmanned Warrior 2016:**

- Conduct joint operations with US-UK Slocum gliders
- Demonstrate near real-time data sharing between USN and RN
- Explore Command and Control aspects with other UUVs

**OFFICE OF NAVAL RESEARCH** www.onr.navy.mil

*Approved for Public Release*

**תקשורת לווינית באמצע האוקיינוס**

בעומק של עשרות מטרים מתחת לפני ים סין הדרומי, אוסטרליה או מפרץ מקסיקו, נע לאיטו גליל צהוב באורך כשני מטרים. בגרסאות מסוימות ללא מנוע, באחרות, באופן משולב. הוא צולל ומרחף באמצעות שינוי עדין של ה-Buoyancy (כוח הציפה) שלו, ומנצל את כוח הכבידה כדי להחליק קדימה כמו דאון תת-ימי. זהו Slocum Glider, רחפן ים אוטונומי (AUGV – Autonomous Underwater Gliding Vehicle) מתוצרת Teledyne Webb Research. הוא יכול להישאר בים חודשים, ולאסוף נתונים אוקיינוגרפיים שמזינים מחקר אקלים, ביטחון ימי וניווט.

כל כמה שעות הוא עולה לפני השטח, שולף אנטנה זעירה, ומחייג הביתה דרך לוויין Iridium. בצד השני של השיחה ממתין שרת חופי בשם Dock Server – לב המערכת ה-Glider Mission Control (GMC), שהיא תוכנת ה-Command and Control של כלי השיט התת ימיים. דרכה מתכנן החוקר את המשימה, מוריד את הנתונים, ושולח Waypoints (נקודות ציון לניווט) חדשים.

המחקר שביצעתי מצא שחלק מאותם "בתים" שאליהם הרחפנים חייגו היו פתוחים לרווחה. הרחפנים הימיים, כולל המחשב שבכלי השיט והמחשב המדעי שבו היו פרוצים, והארכיטקטורה כולה שבורה מבחינה אבטחתית.

6. Power on the modem, Freewave, and laptop in any order.

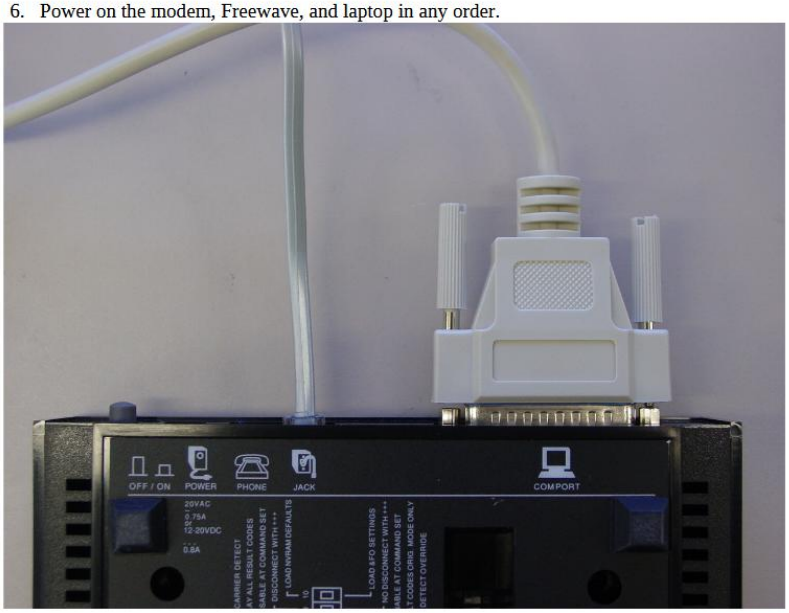
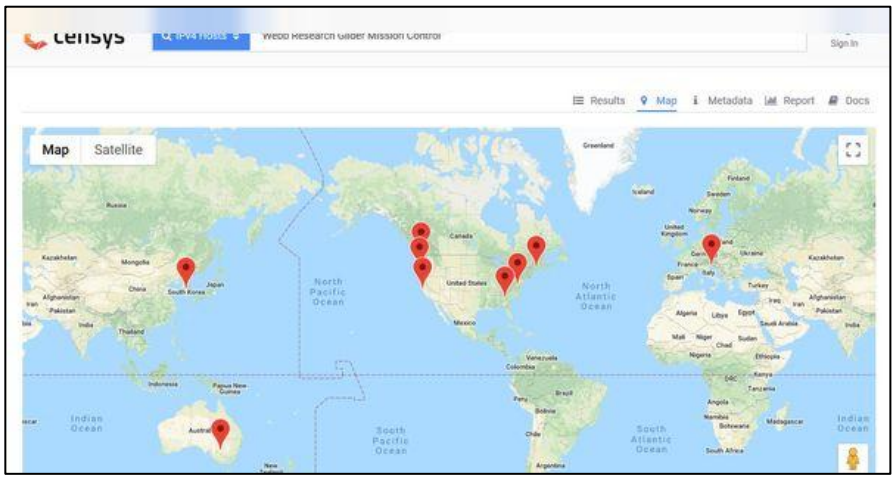



**Figure 1-1. Modem connections to the computer's serial port and iridium phone line.**



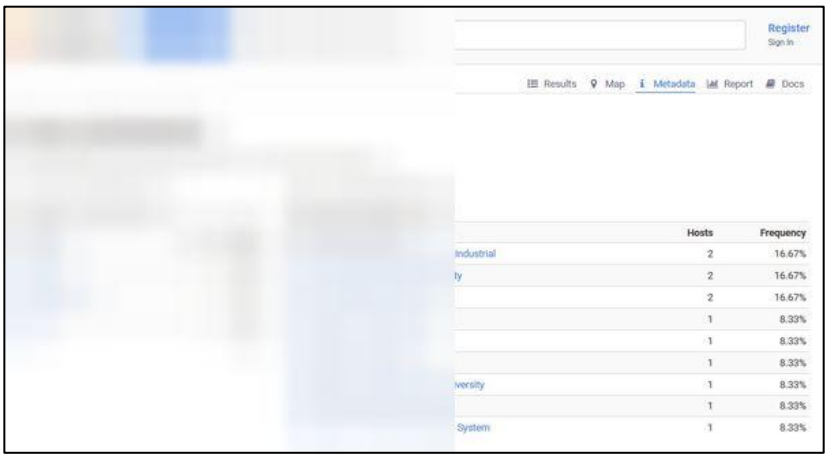

## ממצאים, ניתוח והמלצות

**איך מוצאים צי תת ימי של כלי מחקר**

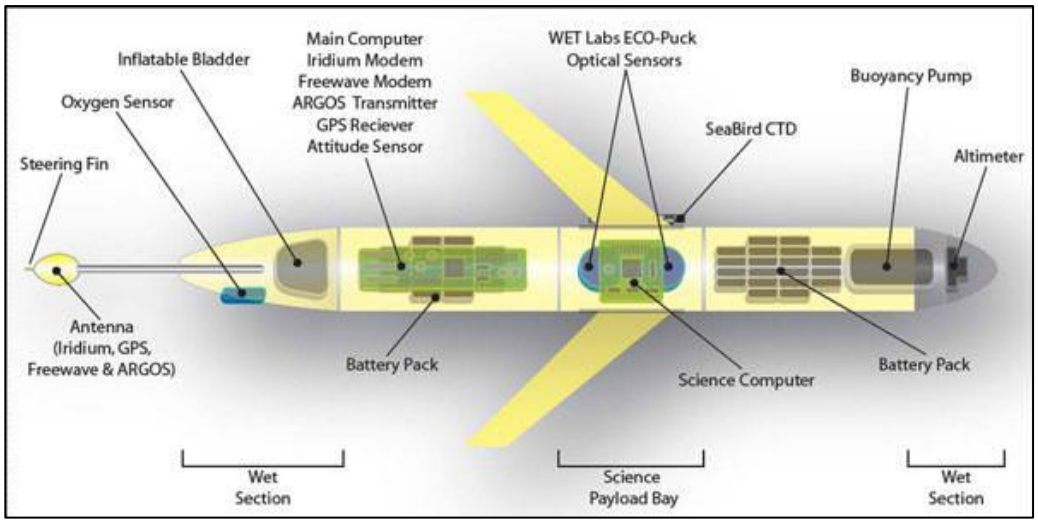
נקודת הפתיחה החלה כאתגר: למדתי על מערכות שליטה ובקרה של משימות חלל, משם המשכתי לכלים על פני הים ולאחר מכן התחלתי לחקור את התווך התת ימי.

הבנתי שהתקשורת הלווינית היא נדבך מרכזי בכל משימה לטווח ארוך, וכך החל מיפוי דליפות אפשריות של תקשורת לווינית, ומשם איתרתי דאון ימי ראשון. חיפוש של מחרוזת הטקסט "Webb Research Glider Mission Control" הוזנה למנועי החיפוש ולפלטפורמות סריקת אינטרנט המתמחות בזיהוי מכשירים מחוברים: Shodan, Censys, ZoomEye ו-FOFA. המנוע Censys לבדו החזיר 12 כתובות IPv4 ייחודיות. הצלבה עם Google Dorks נוספים כמו "GLMPC Terminal" ו-"Glider Terminal" הרחיבה את הרשימה.

התמונה שהתקבלה: **יותר מ-13 שרתי Dock Server פעילים, בשש מדינות, ניהלו יחד מעל 25 רחפני מחקר.** ארצות הברית הובילה עם כמחצית מהשרתים, ולצידה אוסטרליה, דרום קוריאה, ניו זילנד, קנדה ואיטליה.



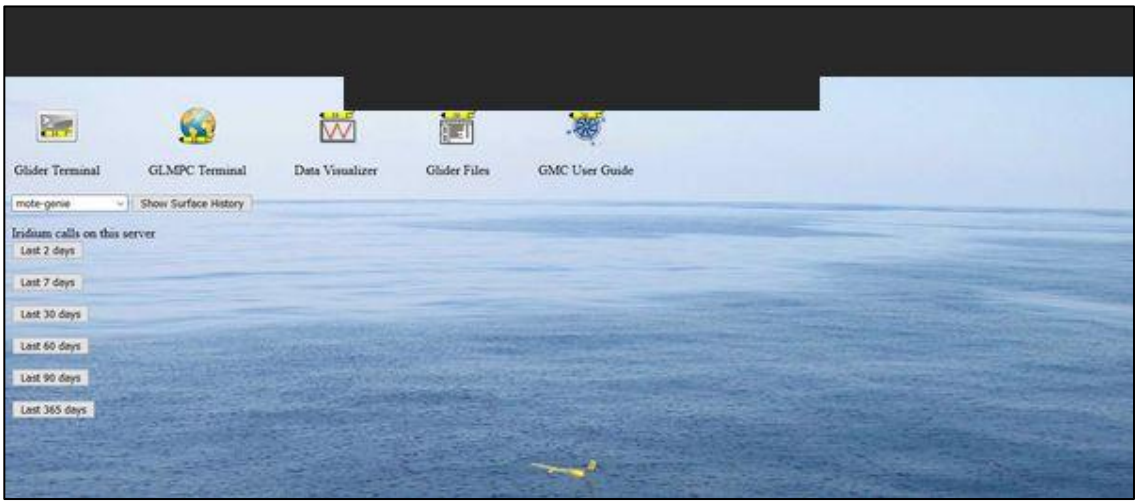

בין הארגונים שזוהו: ה-CSIRO באוסטרליה (סוכנות המדע הלאומית), Mote Marine Laboratory בפלורידה, Oregon State University, ה-Skidaway Institute של אוניברסיטת ג'ורג'יה, Kyungpook National University בדרום קוריאה, ורשת המחקר REANNZ בניו זילנד. שמות הרחפנים שהיו גלויים כללו כינויים מעניינים כמו mote-genie, kg_557, unit_416, ramses, pelagia, bob.

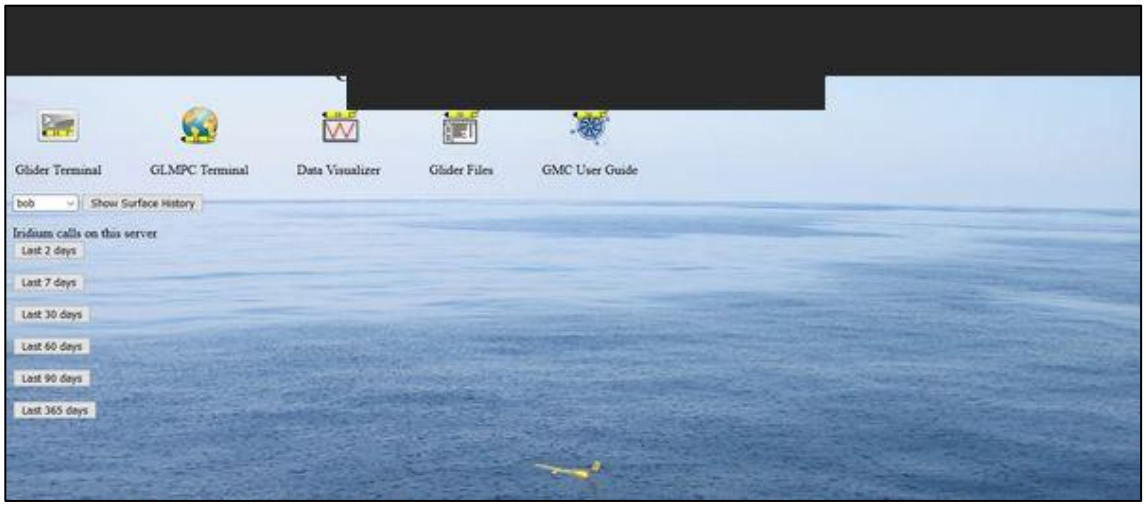



**גישה ללא הגבלה**

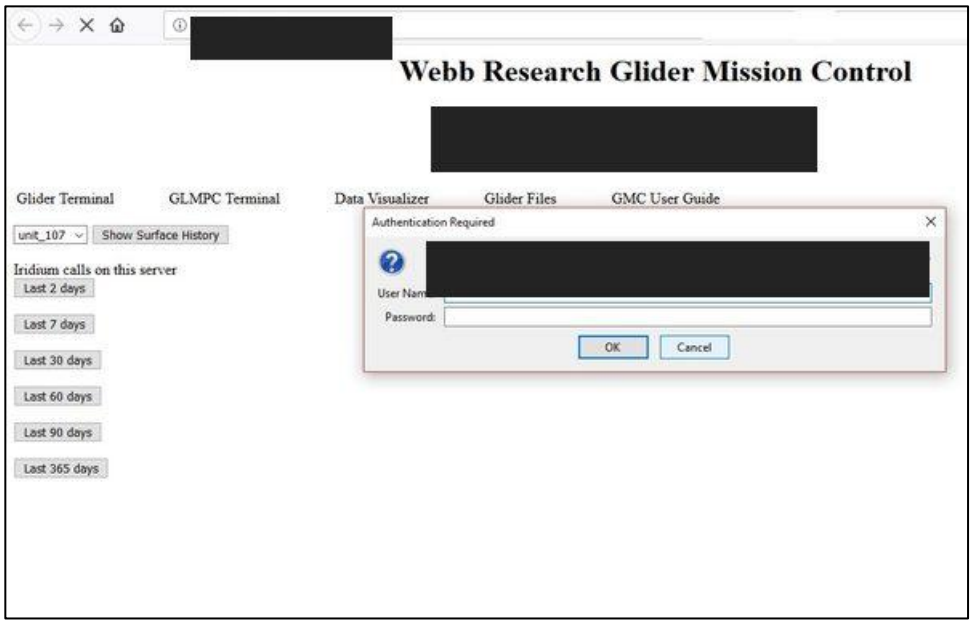
הממצא החמור ביותר הוא גם הפשוט ביותר: 12 מתוך 13 השרתים לא דרשו Authentication כלשהו. לא שם משתמש, לא סיסמה, לא Token. מי שהקליד את הכתובת בדפדפן קיבל גישה מלאה לקונסולת השליטה: רשימת הרחפנים, היסטוריית העליות לפני הים, יומני שיחות הלוויין, וכפתורי הפעלה של כלי השליטה כלי השיט - כולם בממשק מאוחד קל לתפעול.


אותה תמונה חזרה על עצמה ביבשות שונות. לדוגמא: בשרת של Mote Marine Laboratory בפלורידה, ניהל הממשק את הרחפן mote-genie ללא הגנה. שרת הגיבוי של Oregon State University התנהל באופן דומה, וגם כשהחיבור עצמו היה ב-HTTPS, האימות פשוט לא היה קיים. רק שרת אחד ביקש שם משתמש וסיסמא, שיתכן וגם הם היו ברירת מחדל של היצרן.






העיצוב הזה אינו תקלה אקראית. הוא משקף שילוב תרבות אקדמית של שיתוף מידע פתוח שבעבר הייתה גישה לגיטימית במחקר, אך כאן הייתה גישה בלתי הולמת בעליל, כשמערכות אשר שולטות בנכסים פיזיים ששטים בים, שהינם בעלי שימושים ביטחוניים ודו שימושיים, הייתה פתוחה לחלוטין. רק שרת אחד, שייך לגוף אקדמי בארצות הברית, הציב מחסום: HTTP Basic Authentication פשוט עם ההודעה " Restricted Files". החברה המפתחת פיתחה מוצרים בגישה מחקרית שלפיה אבטחה איננה דרישת סף אלא המלצה בלבד והעובדות דיברו בעד עצמן, לקוחות בחרו להתקין את המערכות ללא אבטחה מינימלית.



**תקשורת לווינית**

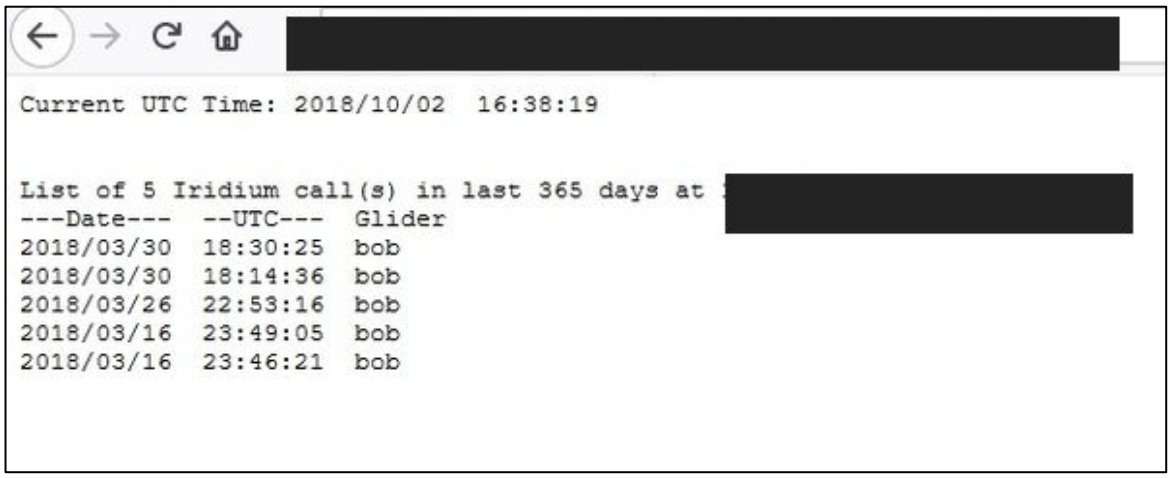
גם השרת הלוויני לא היה מוגן באמת. לצד ממשק ה-Web, שרת זה חשף API פתוח לחלוטין שמחזיר את יומן שיחות ה-Iridium המלא בלי שום אימות:

```
http://<server>/cgi-bin/gmc/list-iridium-results.pl?time=365
```

הפרמטר time מקבל מספר ימים אחורה. החזרה: רשימה כרונולוגית של כל אירוע עלייה לפני השטח, שם הרחפן, חותמת זמן מדויקת לשנייה, ומשך השיחה. עבור גורם עוין זהו אוצר מודיעיני: Operational Tempo (קצב הפעילות), דפוסי תזמון, ומשך הפריסה. בהצלבה עם יומני האירועים גם מיקום GPS.

```
List of 17 Iridium call(s) in last 365 days
---Date---  --UTC---  Glider
2018/09/04  00:16:24  unit_416
2018/09/04  00:03:29  unit_416
2018/09/03  02:05:05  unit_416
2018/08/28  01:53:05  unit_190
2018/08/24  00:48:32  unit_416
2018/08/23  23:24:55  unit_416
2018/08/23  23:14:12  unit_416
2018/08/22  06:46:10  unit_416
2018/08/22  05:42:53  unit_416
2018/08/22  05:31:59  unit_416
2018/08/22  05:15:49  unit_416
2018/08/22  05:13:22  unit_416
2018/08/21  04:12:59  unit_416
2018/08/21  04:08:16  unit_416
2018/08/21  02:35:46  unit_416
2018/08/20  05:57:17  unit_416
2015/07/30  02:41:23  unknown
```

שרת ה-Skidaway Institute של אוניברסיטת ג'ורג'יה שיתף מידע אחר: 1,770 שיחות בשנה אחת. ניתוח של הרחפן pelagia חשף שהוא עלה לפני השטח כמעט כל שבע דקות לאורך תקופה ממושכת – חתימה ברורה של Pitch Mechanism Failure (כשל במנגנון הטיית הגובה). תקלה זהה כמעט נצפתה בניתוח יומני הרחפן kg_557 בדרום קוריאה: שגיאות "pitch not commanded" שחזרו ברציפות במשך שבעה ימים. שני הכשלים היו גלויים לכל צופה מזדמן או גורם שרוצה לדעת מאיפה לאסוף כלי עם טכנולוגיות דו שימושיות.




**מערכת קבצים חשופה**

אם ממשק ה-Web היה דלת ללא מנעול, שרת ה-FTP היה קיר זכוכית. כלי ה-GMC FTP Utility – שמבוסס על תוכנה בשם FTP-Go v1.6 – התחבר ל-Dock Server דרך Plaintext FTP: בלי הצפנה, בלי SFTP, בלי TLS. כל מי שיושב על הנתיב הרשתי רואה את האישורים ואת הנתונים זורמים בטקסט גלוי.

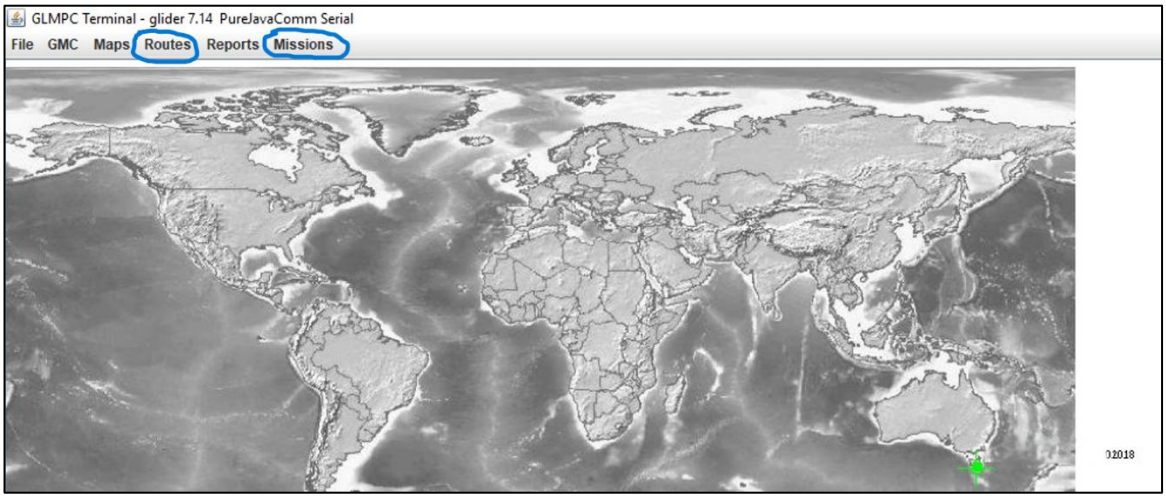
מה שנחשף ב-FTP Root הוא המערכת כולה:

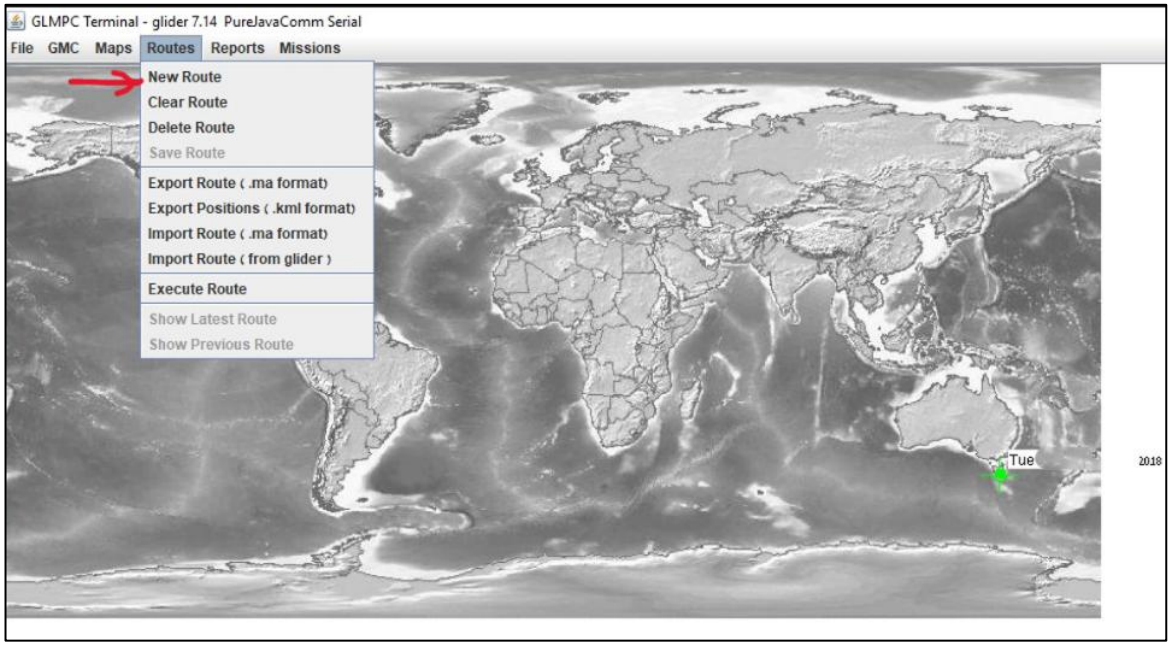
- קבצי Mission בפורמט .ma בתיקיית /to-glider/ – שניתן להעלות ולשנות בהם Waypoints והתנהגויות של רחפן שנמצא כרגע בים
- נתוני המדע הגולמיים: /from-science/ ,/from-glider/
- dockserver.conf – קובץ ה-Configuration של השרת, בטקסט גלוי
- gliderState.xml – מצב הרחפן בזמן אמת, מעל 100 KB

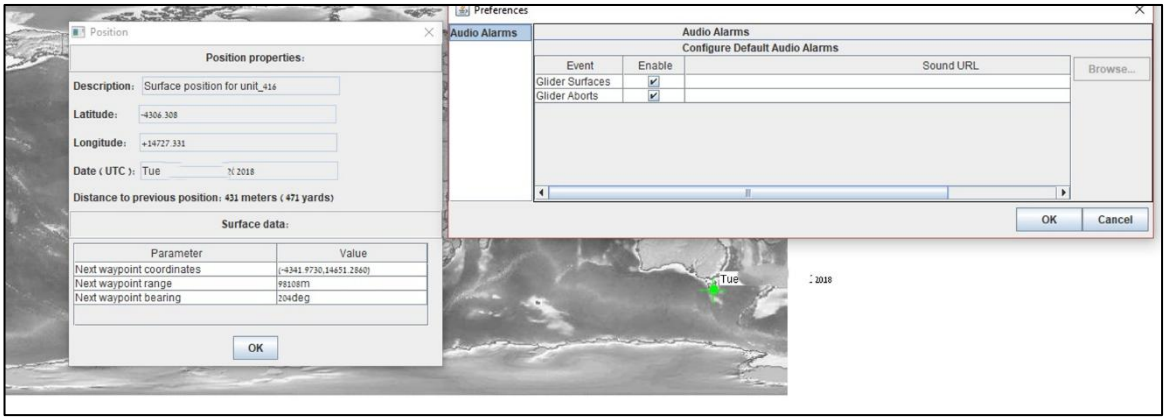
surface.dat – יומני רשת מפורטים לכל אירוע עלייה

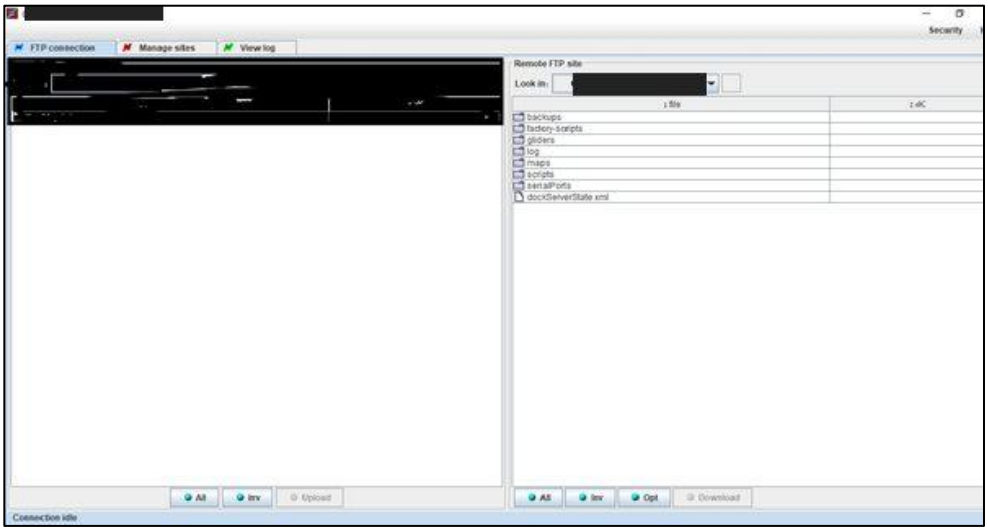
**תופסים את הסיפון - Routes and Missions**

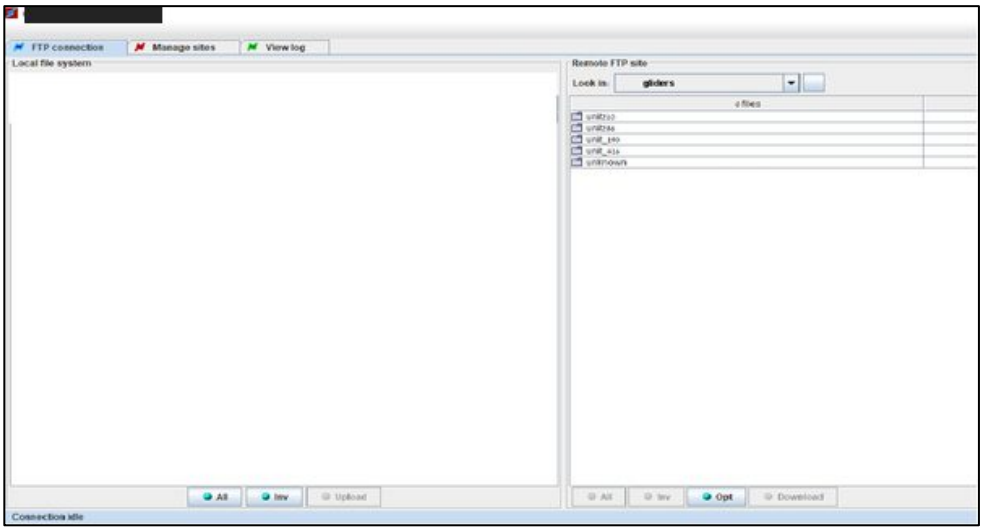
בניגוד לתקיפה ופגיעה בנתוני מחקר או בתפקוד הכלי, כאן הממשק אפשר לקבוע לאן הכלי ישוט. תוקף פוטנציאלי יכל להוסיף משימות למחוק ולשנות משימות ישנות, ולשנות נתיבי שיט ולהחליט להיכן הכלי ישוט עכשיו בים, ומה המשימה שלו, לדוגמא לעבור למדינה אחרת ומשם גורם זר יאסוף את הכלי ויבצע הנדסה לאחור .

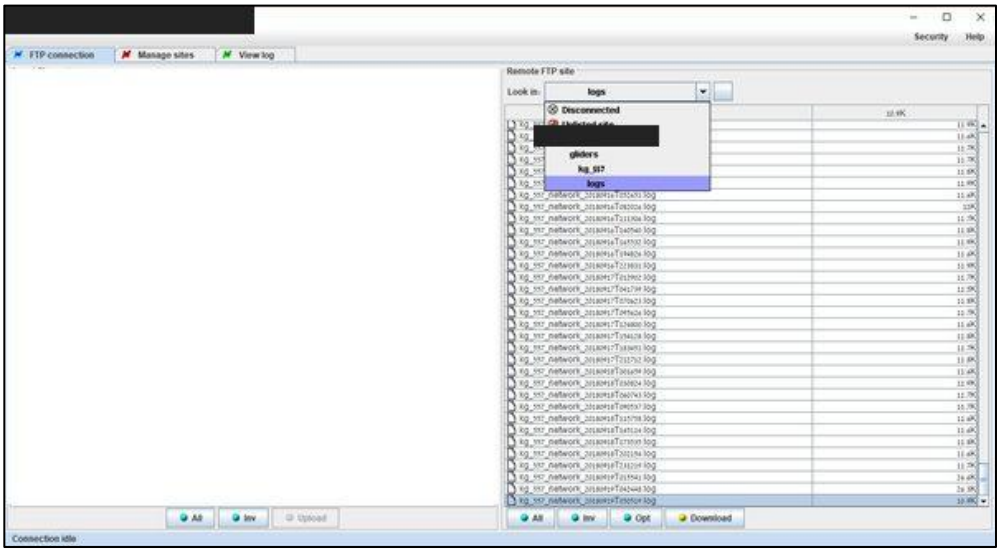

GLMPC Terminal - glider 7.14 PureJavaComm Serial
File GMC Maps Routes Reports Missions


GLMPC Terminal - glider 7.14 PureJavaComm Serial
File GMC Maps Routes Reports Missions
New Route
Clear Route
Delete Route
Save Route
Export Route ( .ma format)
Export Positions ( .kml format)
Import Route ( .ma format)
Import Route ( from glider )
Execute Route
Show Latest Route
Show Previous Route
Tue


Position
Position properties:
Description: Surface position for unit_416
Latitude: -4306.308
Longitude: +14727.331
Date ( UTC ): Tue
Distance to previous position: 431 meters ( 471 yards)
Surface data:
Parameter
Value
Next waypoint coordinates
Next waypoint range
Next waypoint bearing
98108m
204deg
OK
Preferences
Audio Alarms
Configure Default Audio Alarms
Event
Enable
Sound URL
Glider Surfaces
Glider Aborts
Browse...
OK
Cancel


FTP connection
Manage sites
View log
Security
Remote FTP site
Look in:
backups
factory-scripts
gliders
log
maps
scripts
serialPorts
dockServerState.xml
All
Inv
Upload
Opt
Download
Connection idle


FTP connection
Manage sites
View log
Local file system
Remote FTP site
Look in:
gliders
All
Inv
Upload
Opt
Download
Connection idle


FTP connection
Manage sites
View log
Security
Help
Remote FTP site
Look in:
logs
Disconnected
gliders
kg_557
logs
All
Inv
Upload
Opt
Download
Connection idle

**הורדת והעלאת קוד בלי בדיקה מי שלח אותו והאם הוא נגוע**

כל כלי השליטה - Terminal Glider, Terminal GLMPC, Visualizer Data - מועברים למחשב החוקר כחבילות Java Web Start (JNLP). הבעיה: קובצי ה-JAR עצמם יורדים דרך HTTP רגיל, בלי בדיקה.

```
<security>
  <all-permissions/>
</security>
<j2se version="1.1+"/>
```

המשמעות: תוקף שממוקם על הנתיב הרשתי (Man-in-the-Middle) יכול להחליף את ה-JAR בקובץ זדוני. ה-Java Runtime תריץ אותו עם הרשאות מערכת הפעלה מלאות על תחנת החוקר – התקנת Malware, גניבת אישורים, ומעבר אל הרשת הפנימית של המשתמש: מוסד האקדמאי, מכון המחקר, או גורם רלוונטי אחר. למעשה, Java Web Start כבר הוצא משימוש ב-Java 11 (ספטמבר 2018), כך שהמערכות היו תלויות ב-Java 8 ישן ומלא CVEs.

באופן דומה, ניתן לנסות להעלות קבצים עויינים למחשב השליטה והמחשב המדעי של כלי השיט.

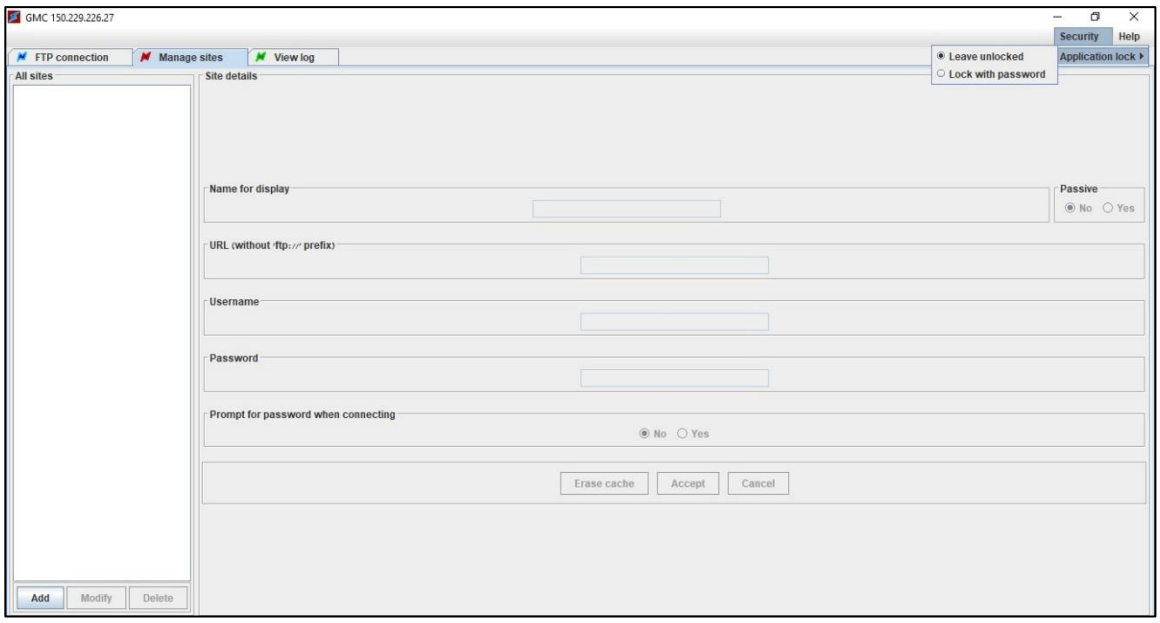
**איך לחסום צוות מחקר שלם בלי שורת קוד אחת**

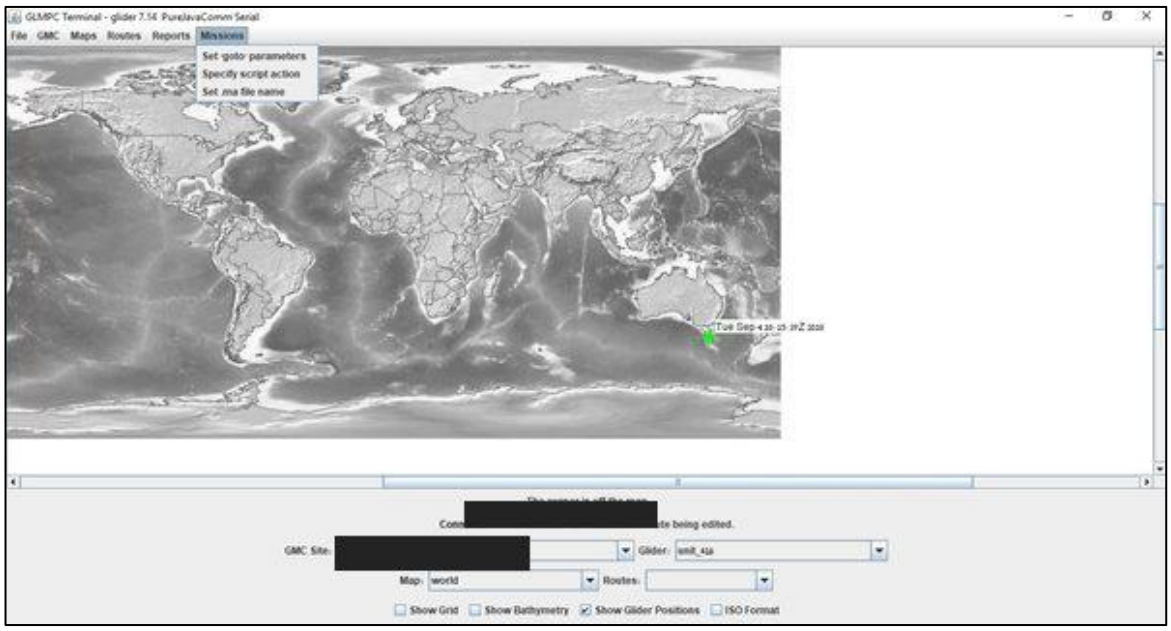
לפעמים הפגיעות מתועדת במו ידי היצרן. ה-Dock Server User Guide (גרסה 7.14, 2013) קובע במפורש:

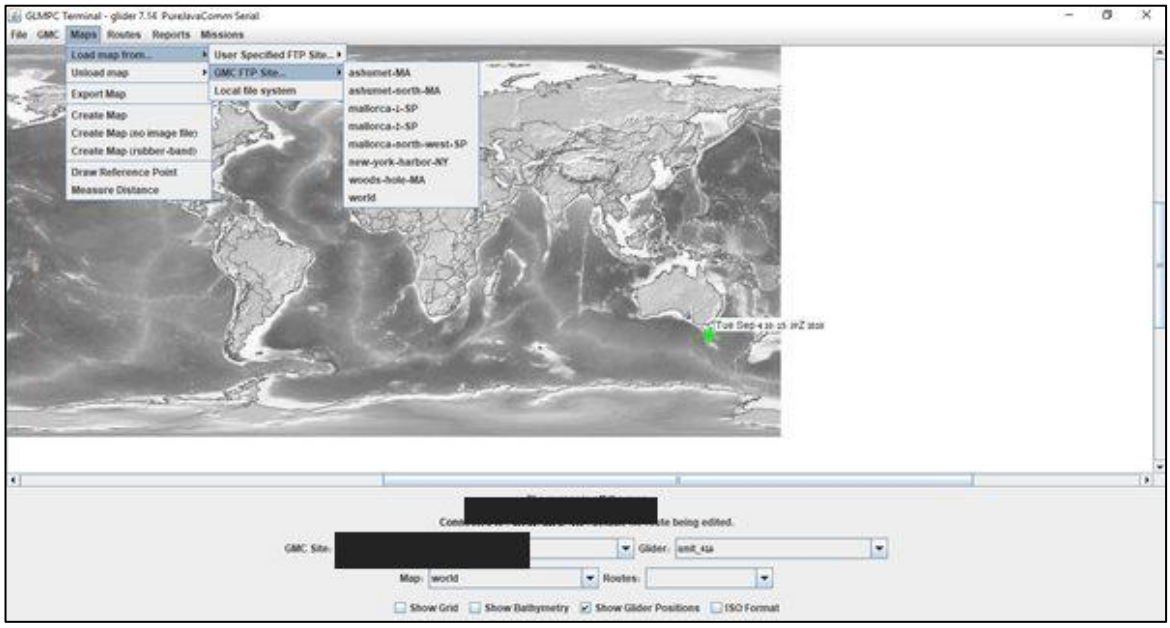
When Dock Server launches, it opens serial ports and network sockets. At any time, these resources can be owned by only a single process... do not start more than one instance.

מכיוון שה-Glider Terminal נגיש ללא Authentication, כל אדם שמתחבר ל-Socket תופס אותו. המפעיל הלגיטימי - צוות המחקר שמנסה לתקשר עם הרחפן שלו - פשוט ננעל בחוץ, לכל משך החיבור של התוקף. זוהי מניעת שירות (DoS) שלמה, ללא Exploit, ללא Malware - רק חיבור TCP.

בנוסף, ניתן היה להוסיף סיסמא בחלק מהממשקים :

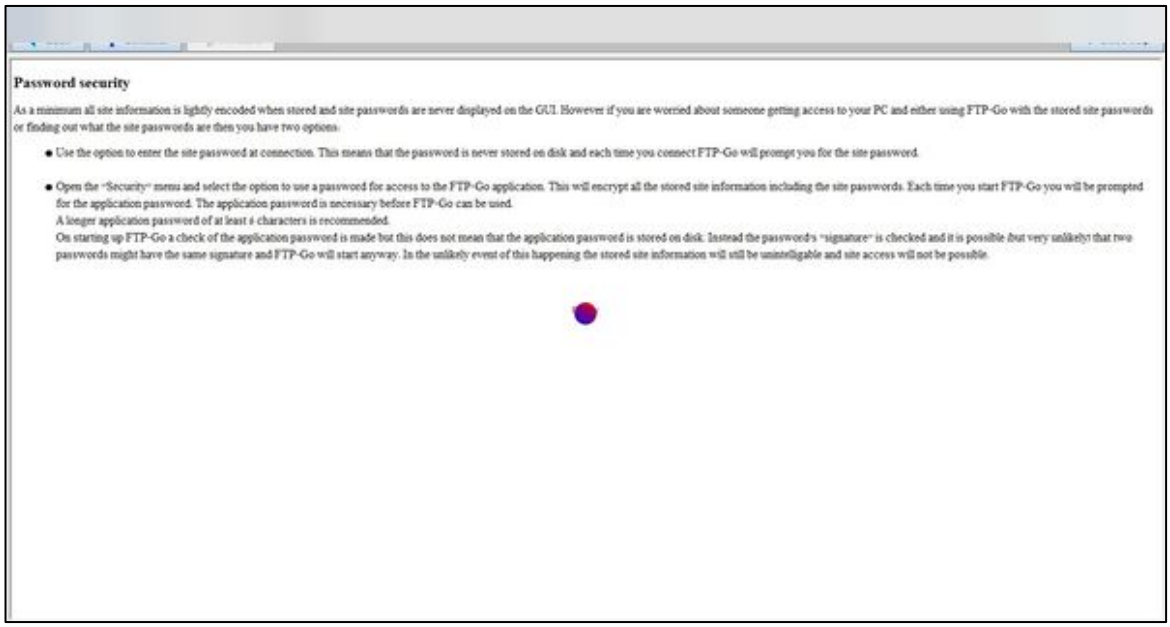





**"קידוד קל" זה לא הצפנה**

גם כשהיו אישורים, הם לא היו בטוחים. התיעוד של FTP-Go מצביע על כך שכל פרטי השרת מאוחסנים ב-"encoding light" קידוד קל, לא הצפנה קריפטוגרפית. בשרת שנבדק (ארגון אוסטרלי) תכונת ה-Application Lock הוגדרה ל-"Leave unlocked". כלומר, כל אישורי ה-FTP לכל ה-Dock Servers שמורים בקובץ שניתן לפענח בקלות, בלי אפילו סיסמה שמגינה על האפליקציה.

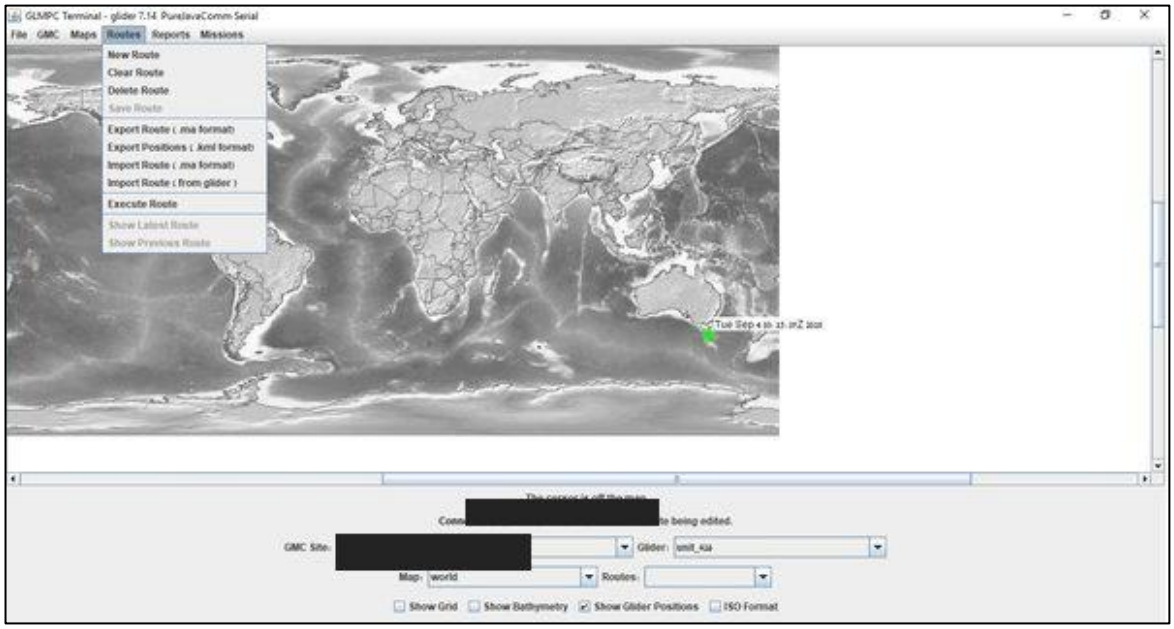


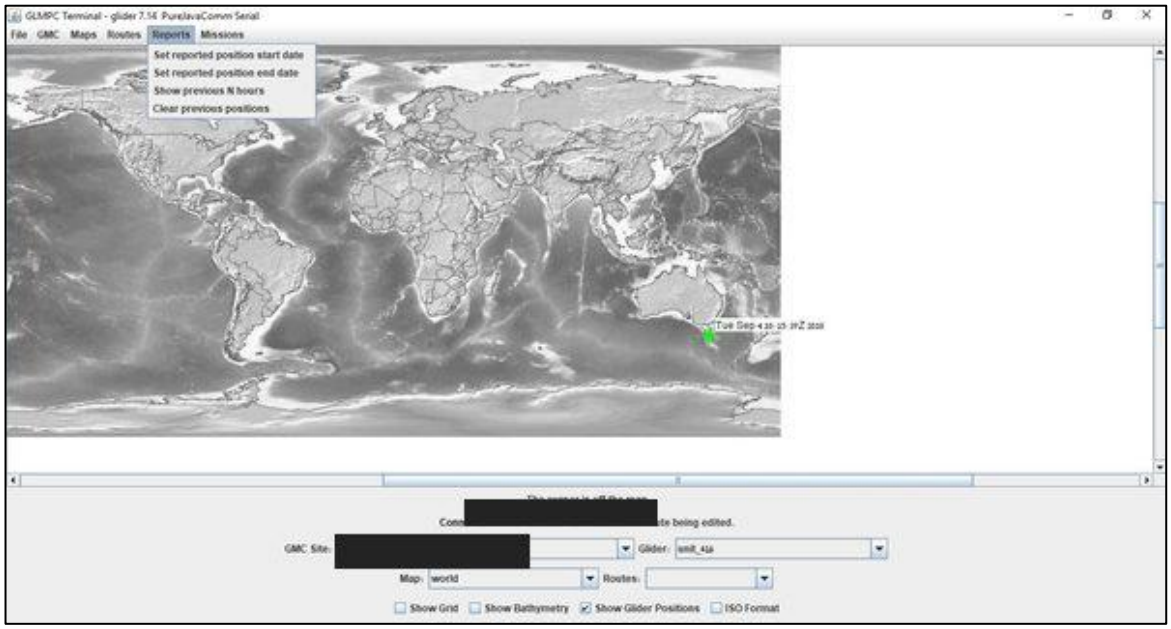
**היכן נמצא כלי השיט התת ימי**

יומני האירועים שמורים על ה-Dock Servers, וכל מי שיש לו FTP יכול להורידם. בתוכם – קואורדינטות GPS מדויקות לכל עלייה, עם חותמת זמן לשנייה.

```
<position dateTime="Wed Aug 22 06:27:32 2018"
      latitude="-4253.266" longitude="14720.184"/>
```

בשילוב עם ה-API של שיחות ה-Iridium, מתקבלת תמונת מעקב בזמן אמת של כל רחפן פרוס – זמינה לכל משתמש אינטרנט, בלי אימות. לאור השימוש ברחפנים אלה באזורים ימיים שונים, זהו סיכון תפעולי שאינו תיאורטי, ומאפשר איסוף של הכלים על ידי גורם חיצוני, כפי שאף התרחש כשסין אספה כלי כזה למטרות לא ברורות.






**סיסמאות ברירת מחדל ופורומים פתוחים**

החקירה מצאה עדויות ל-Factory Credentials שנותרו ללא שינוי ושימוש ב-passwords Hardcoded.

Revision 7.12 1/11/2013

For example, a hostname could be “dock”. A domain name could be “webb.com”. This hostname and domain name would combine to make a fully qualified domain name of “dock.webb.com”.

2. Log on to the Dock Server machine as user “localuser”. The factory delivered password for this account is “WideOpen” (see Appendix D).

### *4.2 Sending Files to a Glider*

To send mission files (mi), mission argument files (ma), or other files to a glider, follow the steps in this section.

1. Transfer the files to the destination glider’s “to-glider” directory on the Dock Server machine.

   For example, to send the mission file lastgasp.mi to glider simbond, transfer the file to the directory /var/opt/gmc/gliders/simbond/to-glider on the Dock Server machine that manages simbond. Any transfer method can be used. Webb supplies the application gmcFTP (section 7.0); however, any FTP client can be used. When using a method other than gmcFTP, use the username “dockserveruser” and password “dockserveruser”.

### 13.5 Dock Server Machine User Accounts

Table 13-5 details the four user accounts related to Dock Server's use as a glider mission control machine. These accounts have different privileges appropriate to their purpose. Refer to Appendix D for the factory delivered passwords to these accounts.

| User Account | Purpose |
|---|---|
| dockserver | The Dock Server application runs as this user. No user login allowed. |
| dataserver | The Data Server application runs as this user. No user login allowed. |
| dockserveruser | Set up for FTP transfer of glider files. The application, gmcFTP, uses this account to FTP files. No user login allowed. |
| localuser | Dock Server user account. All Dock Server control scripts are run from this account – i.e., launch-dockserver, kill-dockserver, see-dockserver, and inspect-dockserver.<br><br>Glider Terminal can be run locally from this account using the |



| | |
|---|---|
| | start-glider-terminal script. |
| root | Dock Server upgrades are run from this account. |

**Table 13-5. Dock Server machine User Accounts.**

### 14.3.1.3 Glider Authentication

Gliders connecting to a Dock Server via Iridium RUDICS **may optionally** be required to authenticate before being allowed access to the Dock Server. Unless there are overwhelming reasons to require Glider Authentication, it is recommended to **NOT** use this capability.
It is difficult enough to communicate with an at sea Glider without the additional barrier of a login sequence. It raises the probability that an at sea Glider will be incommunicado due to misconfiguration, software error, corrupt file, lost password, etc.
If one elects to require Glider authentication, it applies to ALL gliders making an Iridium RUDICS connection.
If one elects to require Glider authentication,:

(i) All gliders may share the same username/password, or
(ii) Each glider may have a unique individual username/password

The Dock Server Application does NOT do the authentication itself. It utilizes the linux PAM (*Pluggable Authentication Module)* to require the underlying operating system to perform the authentication. As shipped, the Dock Server utilizes a local username/password (*/etc/passwd with Shadow Passwords*) for the authentication. This requires the end user to create the appropriate Glider user account(s) on the Dock Server.
Authentication is NOT restricted to local username/password. Any PAM method (Kerberos,OpenPGP, SAMBA, Radius, LDAP, ...) may be employed.
The creation of user accounts and PAM configuration issues are outside the scope of this document and support is NOT available from Webb Research Corporation. If you don't know how to create a user account, you should not have gliders authenticate. If you can't reconfigure PAM without help, you shouldn't change it.

תרגום חופשי:

"14.3.1.3 אימות דאון (Glider Authentication)

דאונים המתחברים לשרת עגינה דרך אירידיום RUDICS עשויים באופן אופציונלי להידרש לאמת לפני שתורשה להם גישה לשרת העגינה. אלא אם ישנן סיבות מכריעות לדרוש אימות דאון, מומלץ לא להשתמש ביכולת זו.

זה קשה מספיק לתקשר עם דאון בים ללא המחסום הנוסף של רצף התחברות. זה מעלה את ההסתברות שדאון בים יהיה ללא קשר (incommunicado) עקב תצורה שגויה, שגיאת תוכנה, קובץ פגום, סיסמה אבודה, וכו'.

אם מישהו בוחר לדרוש אימות דאון, זה חל על כל הדאונים המבצעים חיבור אירידיום RUDICS.

אם מישהו בוחר לדרוש אימות דאון:

(i) כל הדאונים עשויים לשתף את אותו שם משתמש/סיסמה

(ii) לכל דאון עשוי להיות שם משתמש/סיסמה אישי וייחודי משלו

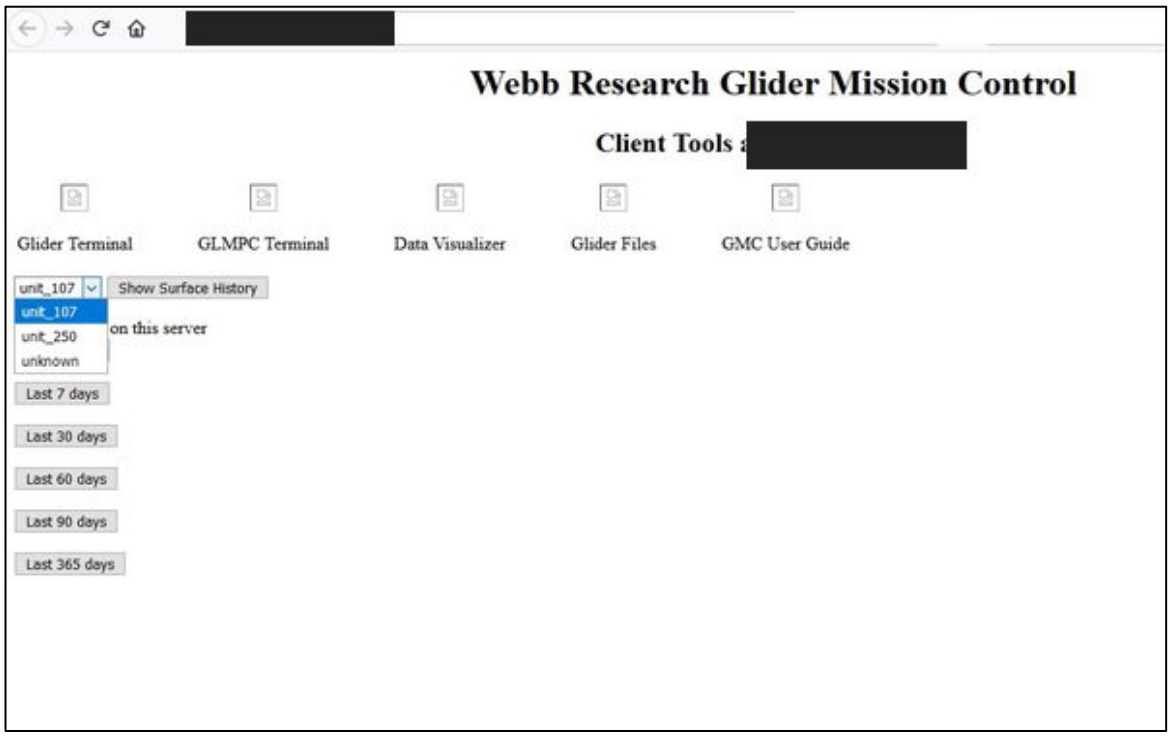
אפליקציית שרת העגינה לא עושה את האימות בעצמה. היא משתמשת ב-PAM ( Pluggable Authentication Module – מודול אימות ניתן לחיבור) של לינוקס כדי לדרוש ממערכת ההפעלה הבסיסית לבצע את האימות. כפי שנשלח, שרת העגינה משתמש בשם משתמש/סיסמה מקומיים (/etc/passwd עם Shadow Passwords) עבור האימות. זה דורש ממשתמש הקצה ליצור את חשבון(ות) משתמש הדאון המתאימים בשרת העגינה.

האימות אינו מוגבל לשם משתמש/סיסמה מקומיים. כל שיטת PAM (Kerberos, OpenPGP, SAMBA, Radius, LDAP, ...) עשויה להיות מופעלת.

היצירה של חשבונות משתמש ונושאי תצורת PAM הם מחוץ להיקף של מסמך זה ותמיכה אינה זמינה מתאגיד Webb Research. אם אתה לא יודע איך ליצור חשבון משתמש, אתה לא צריך להגדיר לדאונים לבצע אימות. אם אתה לא יכול להגדיר מחדש את PAM ללא עזרה, אתה לא צריך לשנות את זה."

[סיום תרגום]

בנוסף, פורום התמיכה הרשמי datahost.webbresearch.com לא כלל קובץ robots.txt, כך שכל דיוני התמיכה הפנימיים ובהם פתרונות תקלות ומידע תפעולי אונדקסו על ידי מנועי החיפוש והיו נגישים דרך השאילתה: site:datahost.webbresearch.com.

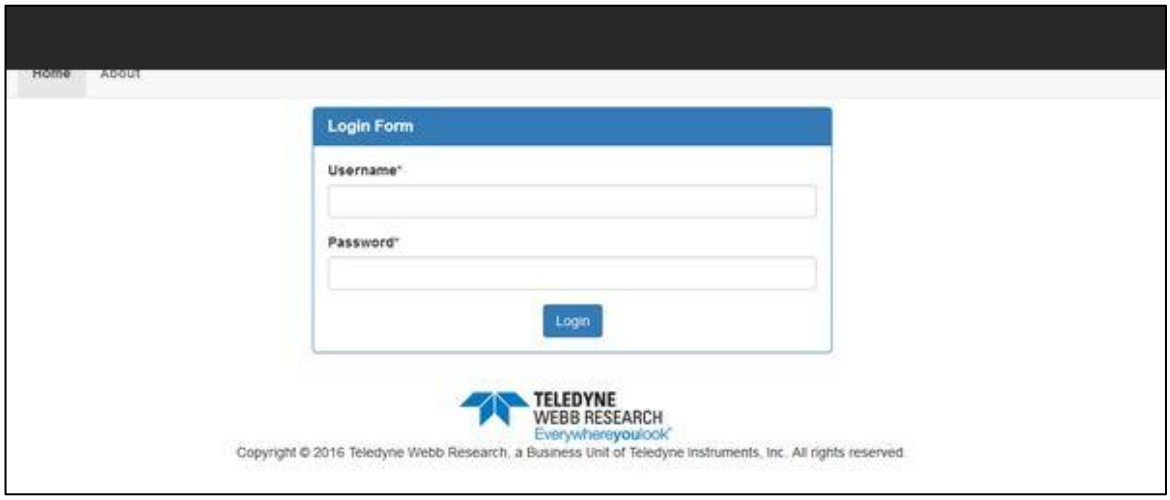


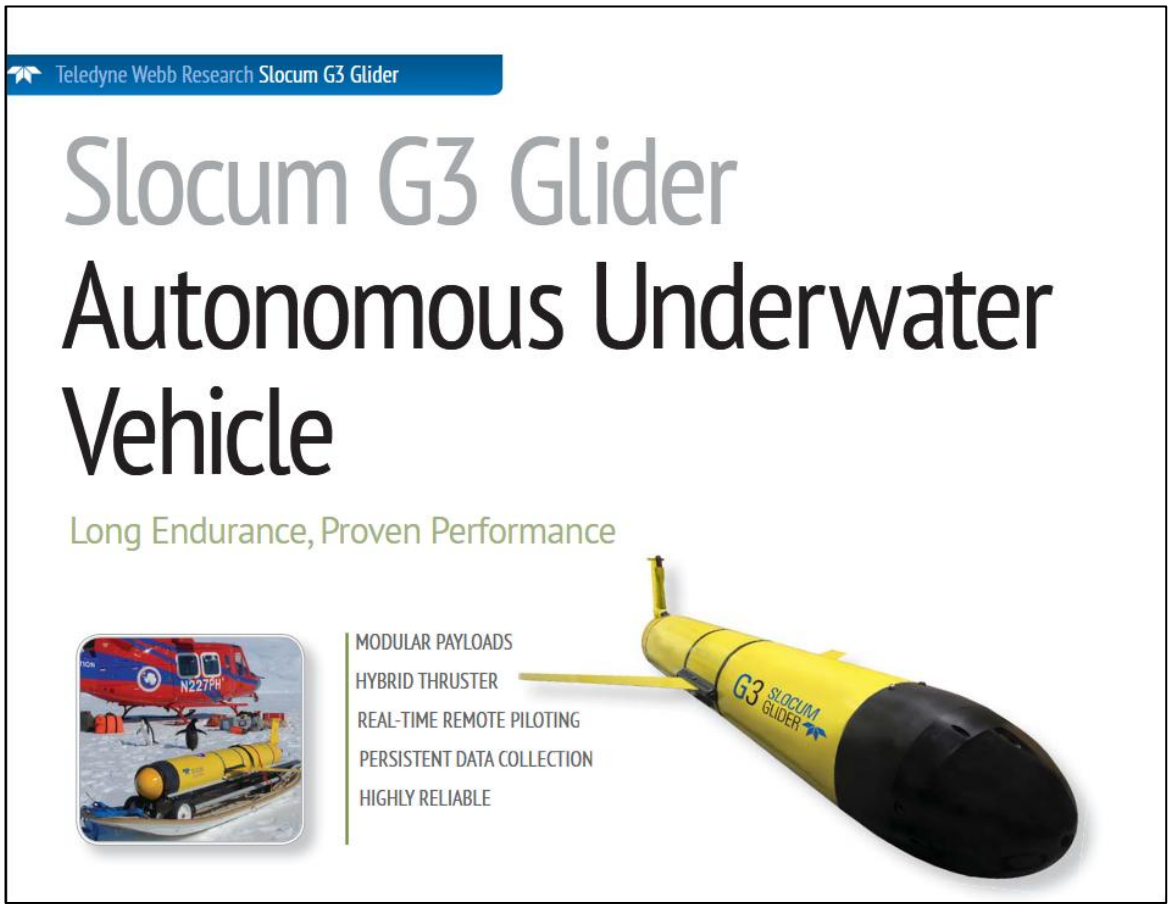


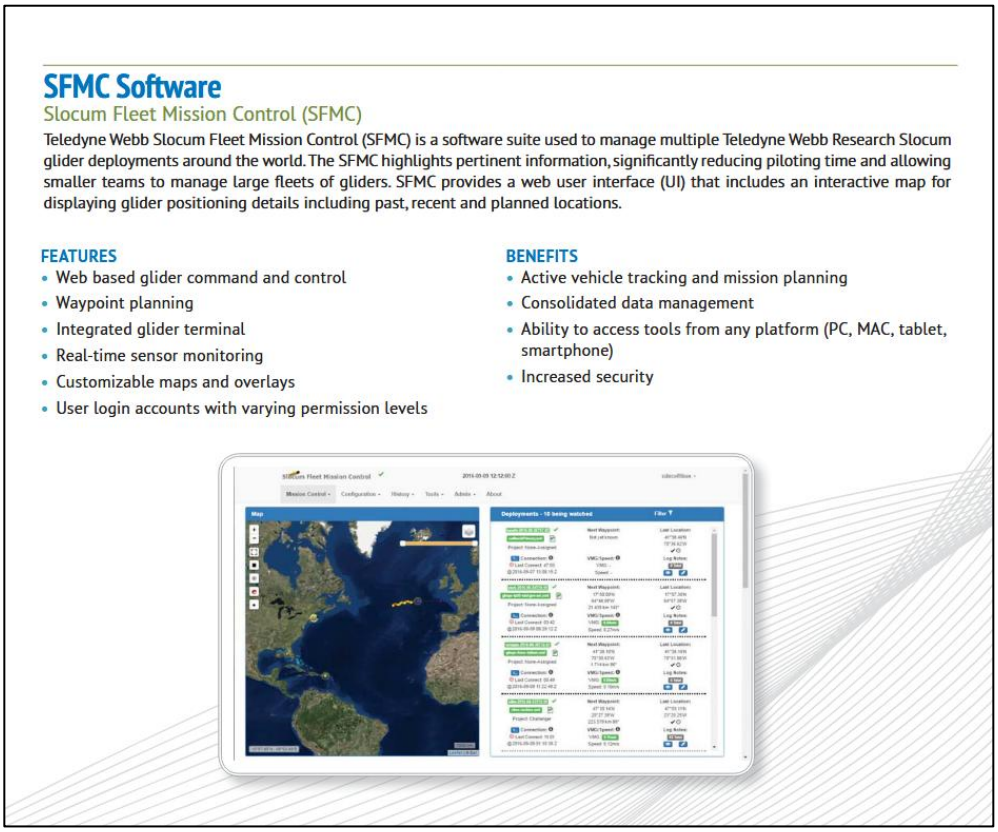
**מערכת שליטה חדשה**

Teledyne Webb Research אכן פיתחה פלטפורמה חדשה, Control Mission Fleet Slocum (SFMC), שכבר משתמשת ב-HTTPS וב-Authentication תקין. מופעים שלה זוהו בתחילת המחקר שביצעתי אצל University of South Florida, Rutgers University, מכון המטאורולוגיה היפני, ואף שרת ההדרכה של החברה עצמה.

קיומו של דור חדש אינו מבטל את הסיכון. 12 ומעלה שרתי GMC מהדור הישן המשיכו לפעול למשך מספר שנים לאחר ההתרעה הראשונית, בלי אימות, במספר מדינות. כל עוד הם היו מחוברים, הצי השקט נשאר חשוף.


Home
About
Login Form
Username*
Password*
Login
TELEDYNE
WEBB RESEARCH
Everywhereyoulook
Copyright © 2016 Teledyne Webb Research, a Business Unit of Teledyne Instruments, Inc. All rights reserved.


Teledyne Webb Research Slocum G3 Glider
Slocum G3 Glider
Autonomous Underwater Vehicle
Long Endurance, Proven Performance
MODULAR PAYLOADS
HYBRID THRUSTER
REAL-TIME REMOTE PILOTING
PERSISTENT DATA COLLECTION
HIGHLY RELIABLE
G3 SLOCUM GLIDER



## SFMC Software

Slocum Fleet Mission Control (SFMC)

Teledyne Webb Slocum Fleet Mission Control (SFMC) is a software suite used to manage multiple Teledyne Webb Research Slocum glider deployments around the world. The SFMC highlights pertinent information, significantly reducing piloting time and allowing smaller teams to manage large fleets of gliders. SFMC provides a web user interface (UI) that includes an interactive map for displaying glider positioning details including past, recent and planned locations.

**FEATURES**

- Web based glider command and control
- Waypoint planning
- Integrated glider terminal
- Real-time sensor monitoring
- Customizable maps and overlays
- User login accounts with varying permission levels

**BENEFITS**

- Active vehicle tracking and mission planning
- Consolidated data management
- Ability to access tools from any platform (PC, MAC, tablet, smartphone)
- Increased security



TELEDYNE MARINE
Everywhereyoulook™

PRODUCT LINES BRANDS MARKET SEGMENTS TECHNOLOGIES

**WEBB RESEARCH**

- APEX Advanced Multi-Sensor Float (AMS)
- APEX Argo
- APEX BioGeoChem
- APEX Current Profiling Float
- APEX Deep
- Batteries - Slocum Glider

## Slocum Fleet Mission Control Software

-Webb Research-

**Key Features:**

- Active Deployment Tracking
- Data Management
- Maps
- Glider Terminal Access
- File Transfers
- Scripts
- User Administration



**עשור, שלושה דורות, ואפס שינוי באבטחה**

מסמכי ה-Operator Manuals הציבוריים פורשים ציר זמן ברור: דור G2 (2010), G1 (2012), מדריך אימון (2014), G3 (2017), ותוכנת GMC גרסה 7.14 (2013). בין כל הדורות הללו לא בוצע שינוי מהותי אחד ב-Security Architecture. פגיעות ה-FTP Plaintext, היעדר ה-Authentication, ומעבר קבצי ה-JARs ב-HTTP כולן קיימות מהגרסה הראשונה ועד האחרונה. מקורות התיעוד: Manual G1 Slocum (2010), G2 Operators Manual (2012), G2 Training Guide (2014), Operators Guidebook (2010), G3 Manual (2017), GMC Dock Server User Guide Rev 7.14 (2013).

**המלצות לתיקון המערכת הישנה**

- Critical – הגבלת ממשק ה-GMC ל-VPN פנימי או רשימת IP מוסדית; הסרת החשיפה לאינטרנט.
- Critical – הטמעת Authentication על כל ה-CGI Endpoints, כולל ה-API של Iridium.
- Critical – החלפה מיידית של כל ה-Default ו-Factory Credentials.
- High – מעבר מ-FTP ל-SFTP או SCP בכל העברות ה-Dock Server.
- High – הגשת כל קובצי JNLP ו-JAR דרך HTTPS עם TLS Certificate תקני.
- High – נטישת Java Web Start (Deprecated) לטובת ממשק Web מודרני ומאומת.
- High – הגבלת חיבורי TCP ל-Socket של ה-Dock Server, עם Authentication.
- Medium – הפעלת Application Lock ב-FTP-Go עם סיסמה חזקה.
- Medium – מדיניות Operational Security לנתוני GPS בזמן אמת.
- Low – הוספת robots.txt לפורום התמיכה.

## סיכום

רחפני ה-Slocum הם הישג הנדסי של מכונות שקטות שחורשות את האוקיינוסים ומחזירות ידע – לוויינים ימיים. אבל ה-Command and Control שלהם נבנה בתפיסה של מעבדה אקדמית פתוחה, לא של מערכת השולטת בנכסים פיזיים בעלי ערך מחקרי. הפער הזה הוא הסיפור.

החברה שפיתחה אותן הטילה אחריות חלקית על הלקוחות תוך המלצה מפורשת לא לאבטח את הכלים עקב חשש לאובדן קשר, בנוסף היא בנתה את המערכת בתצורה שאיננה לוקחת בחשבון מתודולוגיה של Security by design.

הפניות לחברה נמשכו שנים. שיתוף הפעולה היה מאכזב, וכשהיה - היה טלפוני ולא רשמי, ואחת האמירות המעניינות הייתה שאם יפרצו לכלים נזהה את השינוי בנתיב ונשתלט בחזרה, כי הכלי הזה הינו כמו צב ששט ממש לאט ואי אפשר לפגוע בו. חשוב לציין שהפניה לחברה הייתה אחרי התקרית שבה גורמים סינים תפסו כלי כזה, אך הלקח לא נלמד.

אם רוצים לבצע פגיעה במחקרים אקדמאיים, גניבת סודות מסחריים או כלי מחקר דו שימושיים, תפיסות תמימות אלו הן הבסיס שמאפשרות את זה.

## תהיות לגבי המערכת החדשה

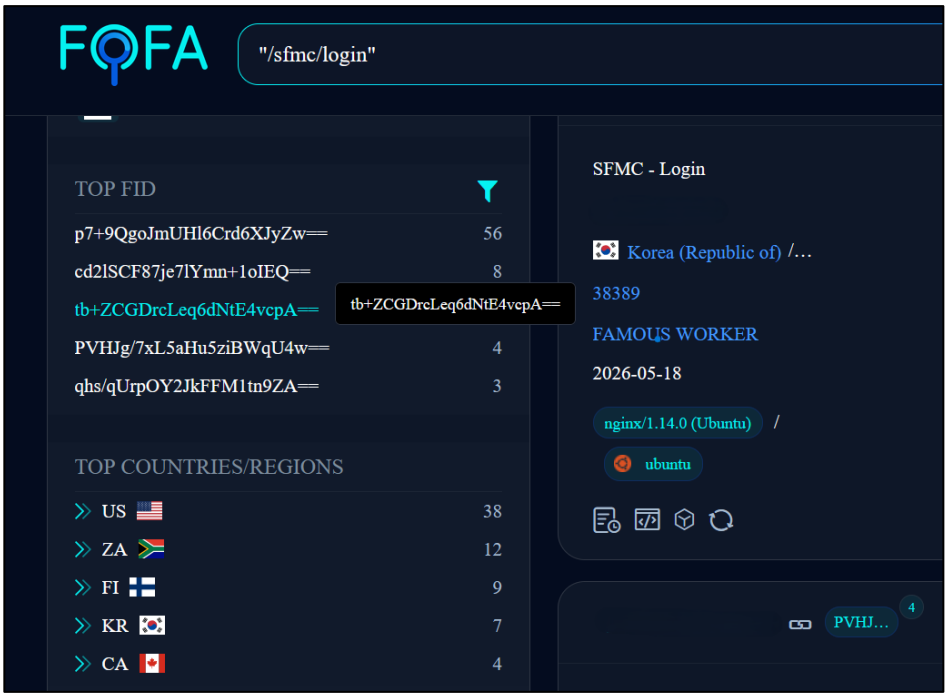
אם תרצו לאתר את הצי החדש והמאובטח, כל מה שתצטרכו זה לחפש את אחד מהצירופים הבאים:

```
"/sfmc/login"  "/sfmc/login" && title=="SFMC - Login" "/sfmc/about"
```

אפשר גם להגיע ללוגים בסיסיים של נתוני לוויין "sfmc/iridium-calls" ללא מיקומים.

העובדה שעשרות לקוחות עדיין חושפים את המערכת לאינטרנט, וכל שנדרש הוא שם משתמש וסיסמא, ללא דרישה גורפת של שימוש ב-VPN ארגוני, מצביעה על כך שמלבד הוספת דרישה לסיסמא בסיסית, ומודרניזציה של המערכת מבחינת אבטחה, אין הרבה שינוי תפיסתי.

מדריכי הפעלה מודרניים שפורסמו מצביעים על שיפור ודרישה להחלפת סיסמאות תקופתית. באיזון בין תפעוליות לאבטחה, נראה שהתפעול עדיין מוביל.




## על המחבר

אמיתי דן – חוקר אבטחת מידע. המאמר נכתב במקור ב-2018 ונערך מחדש לפרסום ב-18.06.2026.

https://x.com/popshark1

http://amitaydan.com

https://il.linkedin.com/in/amitay-dan-a63647aa

**גילוי נאות – Full Disclosure**

פניות אל חברת Teledyne Webb Research בנוגע לממצאים המתוארים במאמר זה הועברו מספר פעמים לאורך שנים. תהליך ה-Remediation (התיקון) התארך באופן ניכר עקב חוסר שיתוף פעולה מצד הגורמים האחראים; חלק מהפגיעויות טרם תוקנו במלואן בעת הפרסום. מירב הלקוחות עדכנו גרסאות ולכן החלטתי לשחרר את המאמר.



פניה ראשונה לחברה נענתה ב-22.09.2018. נלוו לכך אימיילים לגורמים שונים בחברת Webb Teledyne Research כולל שיחה טלפונית ישירה. החברה יידעה ככל הנראה את הלקוחות אך לא הייתה תגובה רשמית ומשתמשים המשיכו להפעיל כלים ימיים באופן לא מאובטח.

פניה נוספת שנעשתה ב-22.01.2024 למחלקת אבטחת מידע לא נענתה.

לאור רגישות הכלים שאינם מחקריים, בחרתי שלא לפרסם את המחקר עד כה.



## מקורות מידע


- Slocum G1 Glider Manual (2010) https://gliderfs.coas.oregonstate.edu/gliderweb/docs/slocum_manuals/Slocum_G1_Glider_Manual.pdf
- Slocum G2 Operators Manual Rev.B (2012) https://gliderfs.coas.oregonstate.edu/gliderweb/docs/slocum_manuals/Slocum_G2_Glider_Operators_Manual.pdf
- Slocum G2 Operators Training Guide (2014) https://gliderfs.coas.oregonstate.edu/gliderweb/docs/slocum_manuals/Slocum_Glider_Operators_Training_Guide.pdf
- Slocum Glider Operators Guidebook (2010) https://wiki-pnb.eri.ucsb.edu/images/f/f2/Glider_operators_handbook.pdf
- Slocum G3 Operators Manual Rev.2 (2017) https://gliderfs.coas.oregonstate.edu/gliderweb/docs/slocum_manuals/Slocum_G3_Operator_Manual_20171219.pdf

- GMC Dock Server User Guide Rev 7.14 (2013)
  https://dockserver.skio.uga.edu/gmc/gmcUserGuide.pdf
- Censys https://censys.io/ipv4?q=%22Webb+Research+Glider+Mission+Control%22
- Shodan
  https://www.shodan.io/search?query=%22Webb+Research+Glider+Mission+Control%22
- ZoomEye
  https://www.zoomeye.org/searchResult?q=%22Webb%20Research%20Glider%20Mission%20Control%22
- TWR Forum
  https://datahost.webbresearch.com
- A Hometown Glider Makes World News
  https://www.capenews.net/falmouth/news/a-hometown-glider-makes-world-news/article_503ef0ab-a95f-5354-8378-7def4f6d3ae1.html
- China Gives Drone Back
  https://www.twz.com/6604/china-gives-drone-back-but-why-did-they-grab-it-in-the-first-place
- Statement by Pentagon Press Secretary
  https://www.war.gov/News/Releases/Release/Article/1032611/statement-by-pentagon-press-secretary-peter-cook-on-incident-in-south-china-sea
- UnitedStates Fleet Forces Command
  https://en.wikipedia.org/wiki/United_States_Fleet_Forces_Command
- Oregon State University - Manuals & Resources, active and archived Deployments 2026
  https://gliderfs2.oce.orst.edu/gliderweb/slocumgliders.php