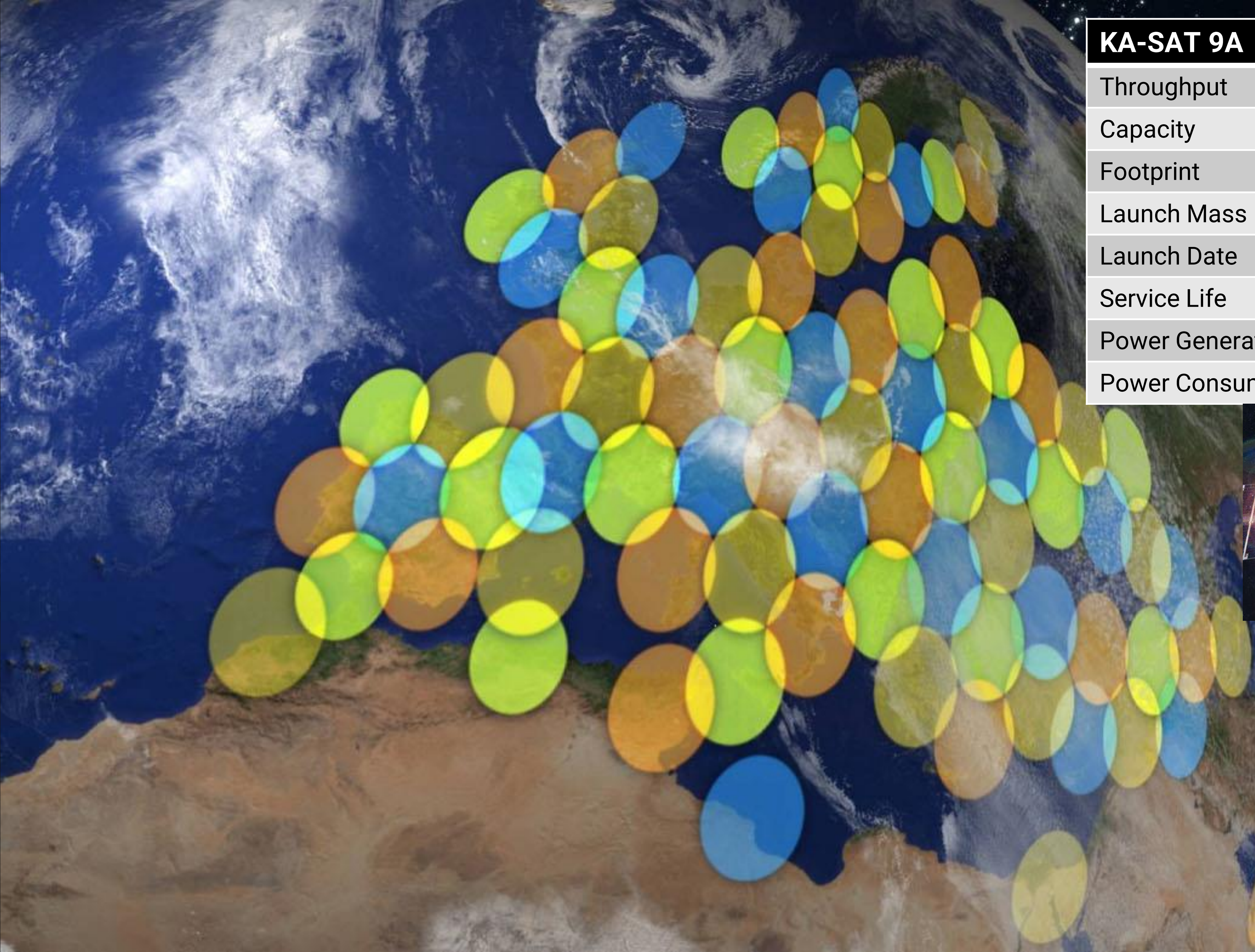
BEARS IN SPACE

SPACE BEARS



KA-SAT 9A

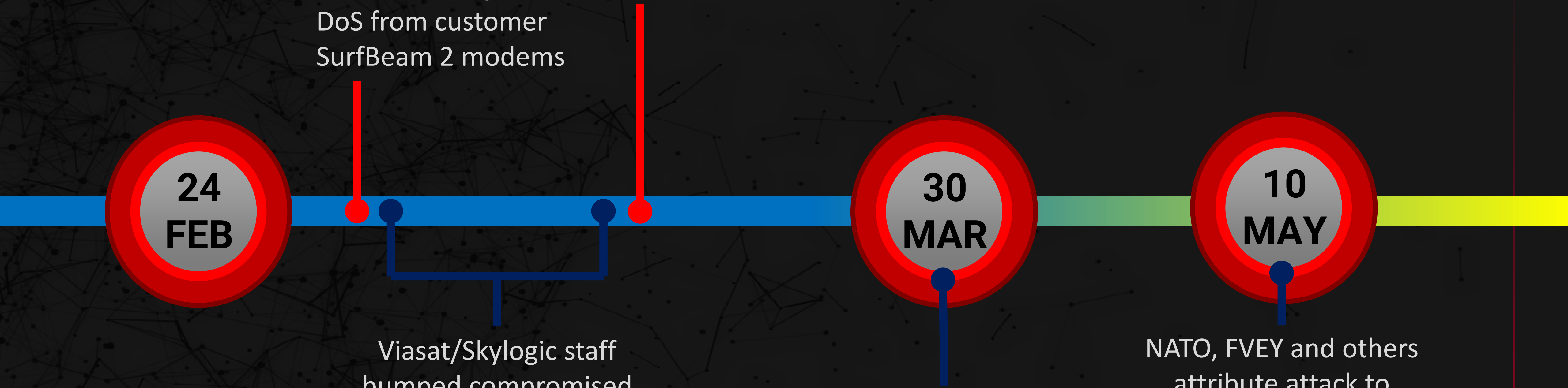
Throughput	Up to 50 Mbps down
Capacity	70-90 Gbps
Footprint	82 spot beams (Ka)
Launch Mass	6.15 metric tons
Launch Date	26 December 2010
Service Life	15 years
Power Generation	15 KW
Power Consumption	11 KW

Russiaball by dykroon-chan @ DeviantArt, Viasat by Viasat

Some Mysterious Time
Exploitation of misconfigured VPN appliance to gain access to management segment

0302h
Viasat user segment DoS from customer SurfBeam 2 modems

0415-0500h (approx)
Large number of customer modems started dropping from network



24 FEB

Viasat/Skylogic staff bumped compromised modems off network

30 MAR

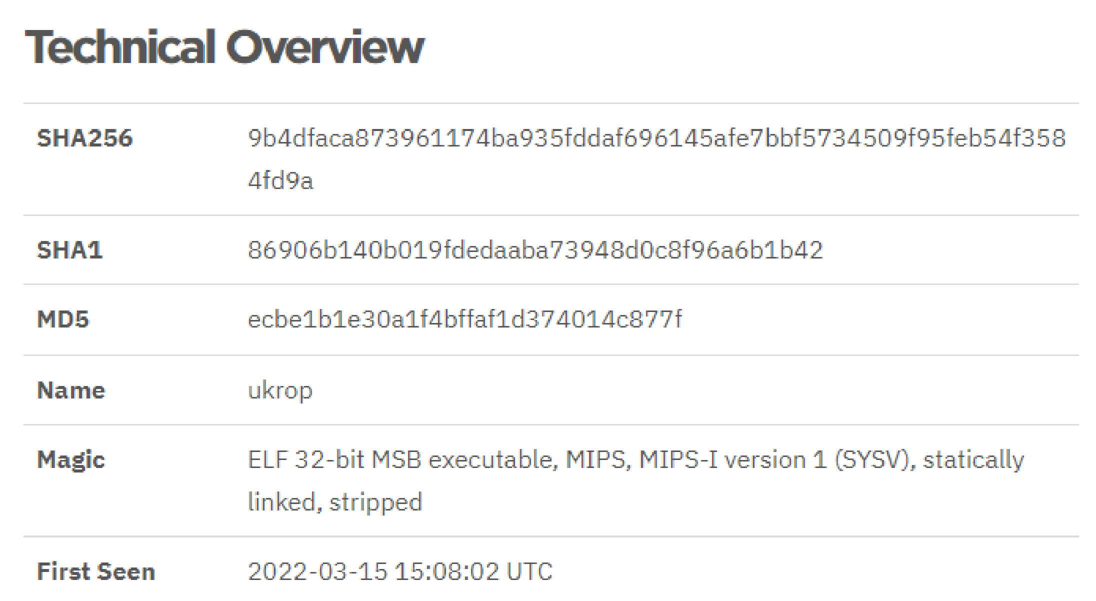
Viasat releases incident summary

10 MAY

NATO, FVEY and others attribute attack to Russia

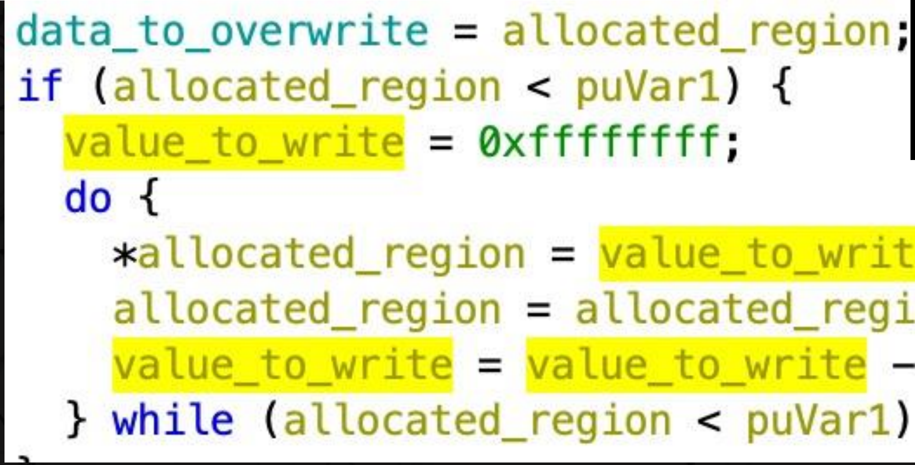
[DESIRE TO KNOW MORE INTENSIFIES]

IT'S RAINING ACID

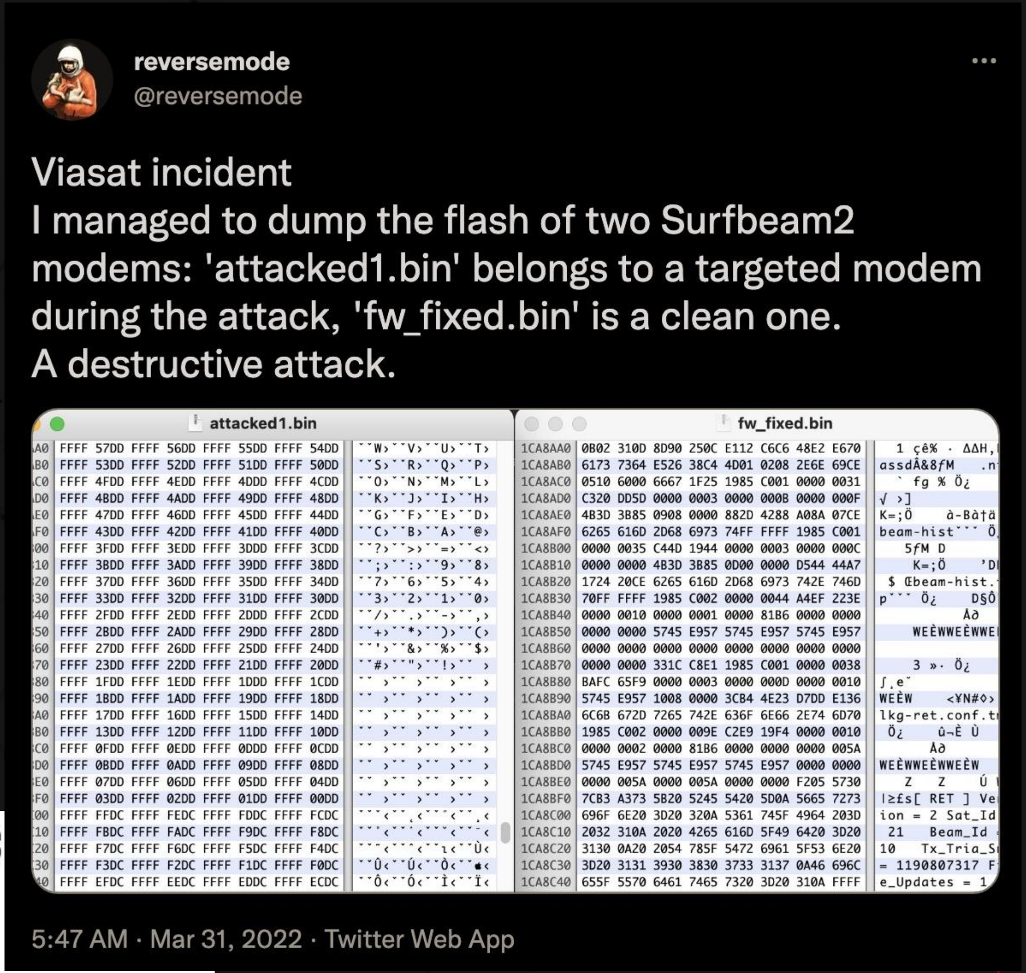


Technical Overview

SHA256	9b4dfaca873961174ba935fddaf696145afe7bbf5734509f95feb54f3584fd9a
SHA1	86906b140b019fdedaaba73948d0c8f96a6b1b42
MD5	ecbe1b1e30a1f4bffaf1d374014c877f
Name	ukrop
Magic	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
First Seen	2022-03-15 15:08:02 UTC



```
data_to_overwrite = allocated_region;
if (allocated_region < puVar1) {
  value_to_write = 0xffffffff;
  do {
    *allocated_region = value_to_write;
    allocated_region = allocated_region + 1;
    value_to_write = value_to_write - 1;
  } while (allocated_region < puVar1);
```



reversemode
@reversemode

Viasat incident
I managed to dump the flash of two Surfbeam2 modems: 'attacked1.bin' belongs to a targeted modem during the attack, 'fw_fixed.bin' is a clean one.
A destructive attack.

attacked1.bin

```
A0  FFFF 57DD FFFF 56DD FFFF 55DD FFFF 54DD
B0  FFFF 53DD FFFF 52DD FFFF 51DD FFFF 50DD
C0  FFFF 4FDD FFFF 4EDD FFFF 4DDD FFFF 4CDD
D0  FFFF 4BDD FFFF 4ADD FFFF 49DD FFFF 48DD
E0  FFFF 47DD FFFF 46DD FFFF 45DD FFFF 44DD
F0  FFFF 43DD FFFF 42DD FFFF 41DD FFFF 40DD
00  FFFF 3FDD FFFF 3EDD FFFF 3DDD FFFF 3CDD
10  FFFF 3BDD FFFF 3ADD FFFF 39DD FFFF 38DD
20  FFFF 37DD FFFF 36DD FFFF 35DD FFFF 34DD
30  FFFF 33DD FFFF 32DD FFFF 31DD FFFF 30DD
40  FFFF 2FDD FFFF 2EDD FFFF 2DDD FFFF 2CDD
50  FFFF 2BDD FFFF 2ADD FFFF 29DD FFFF 28DD
60  FFFF 27DD FFFF 26DD FFFF 25DD FFFF 24DD
70  FFFF 23DD FFFF 22DD FFFF 21DD FFFF 20DD
80  FFFF 1FDD FFFF 1EDD FFFF 1DDD FFFF 1CDD
90  FFFF 1BDD FFFF 1ADD FFFF 19DD FFFF 18DD
A0  FFFF 17DD FFFF 16DD FFFF 15DD FFFF 14DD
B0  FFFF 13DD FFFF 12DD FFFF 11DD FFFF 10DD
C0  FFFF 0FDD FFFF 0EDD FFFF 0DDD FFFF 0CDD
D0  FFFF 0BDD FFFF 0ADD FFFF 09DD FFFF 08DD
E0  FFFF 07DD FFFF 06DD FFFF 05DD FFFF 04DD
F0  FFFF 03DD FFFF 02DD FFFF 01DD FFFF 00DD
00  FFFF FFDC FFFF FEDC FFFF FDDC FFFF FCDC
10  FFFF FBDC FFFF FADC FFFF F9DC FFFF F8DC
20  FFFF F7DC FFFF F6DC FFFF F5DC FFFF F4DC
30  FFFF F3DC FFFF F2DC FFFF F1DC FFFF F0DC
40  FFFF EFDC FFFF EEDC FFFF EDDC FFFF ECDC
```

fw_fixed.bin

```
1CA8AA0  0B02 310D 8D90 250C E112 C6C6 48E2 E670    1 çê% · ΔΔH,
1CA8AB0  6173 7364 E526 38C4 4D01 0208 2E6E 69CE  assdÂ&8ƒM    .n
1CA8AC0  0510 6000 6667 1F25 1985 C001 0000 0031     ` fg % Ö¿
1CA8AD0  C320 DD5D 0000 0003 0000 000B 0000 000F  √ ›]
1CA8AE0  4B3D 3B85 0908 0000 882D 4288 A08A 07CE  K=;Ö    à-Bà†ä
1CA8AF0  6265 616D 2D68 6973 74FF FFFF 1985 C001  beam-hist˘˘˘ Ö
1CA8B00  0000 0035 C44D 1944 0000 0003 0000 000C     5ƒM D
1CA8B10  0000 0000 4B3D 3B85 0D00 0000 D544 44A7      K=;Ö    'D
1CA8B20  1724 20CE 6265 616D 2D68 6973 742E 746D   $ Œbeam-hist.
1CA8B30  70FF FFFF 1985 C002 0000 0044 A4EF 223E  p˘˘˘ Ö¿     D§Ô
1CA8B40  0000 0010 0000 0001 0000 81B6 0000 0000             Å∂
1CA8B50  0000 0000 5745 E957 5745 E957 5745 E957      WEÈWWEÈWWE
1CA8B60  0000 0000 0000 0000 0000 0000 0000 0000
1CA8B70  0000 0000 331C C8E1 1985 C001 0000 0038      3 »· Ö¿
1CA8B80  BAFC 65F9 0000 0003 0000 000D 0000 0010  ∫¸e˘
1CA8B90  5745 E957 1008 0000 3CB4 4E23 D7DD E136  WEÈW     <¥N#◊›
1CA8BA0  6C6B 672D 7265 742E 636F 6E66 2E74 6D70  lkg-ret.conf.t
1CA8BB0  1985 C002 0000 009E C2E9 19F4 0000 0010   Ö¿     û¬È Ù
1CA8BC0  0000 0002 0000 81B6 0000 0000 0000 005A           Å∂
1CA8BD0  5745 E957 5745 E957 5745 E957 0000 0000  WEÈWWEÈWWEÈW
1CA8BE0  0000 005A 0000 005A 0000 0000 F205 5730     Z   Z     Ú
1CA8BF0  7CB3 A373 5B20 5245 5420 5D0A 5665 7273  |≥£s[ RET ] Ve
1CA8C00  696F 6E20 3D20 320A 5361 745F 4964 203D  ion = 2 Sat_Id
1CA8C10  2032 310A 2020 4265 616D 5F49 6420 3D20   21   Beam_Id
1CA8C20  3130 0A20 2054 785F 5472 6961 5F53 6E20  10   Tx_Tria_S
1CA8C30  3D20 3131 3930 3830 3733 3137 0A46 696C  = 1190807317 F
1CA8C40  655F 5570 6461 7465 7320 3D20 310A FFFF  e_Updates = 1
```

5:47 AM · Mar 31, 2022 · Twitter Web App

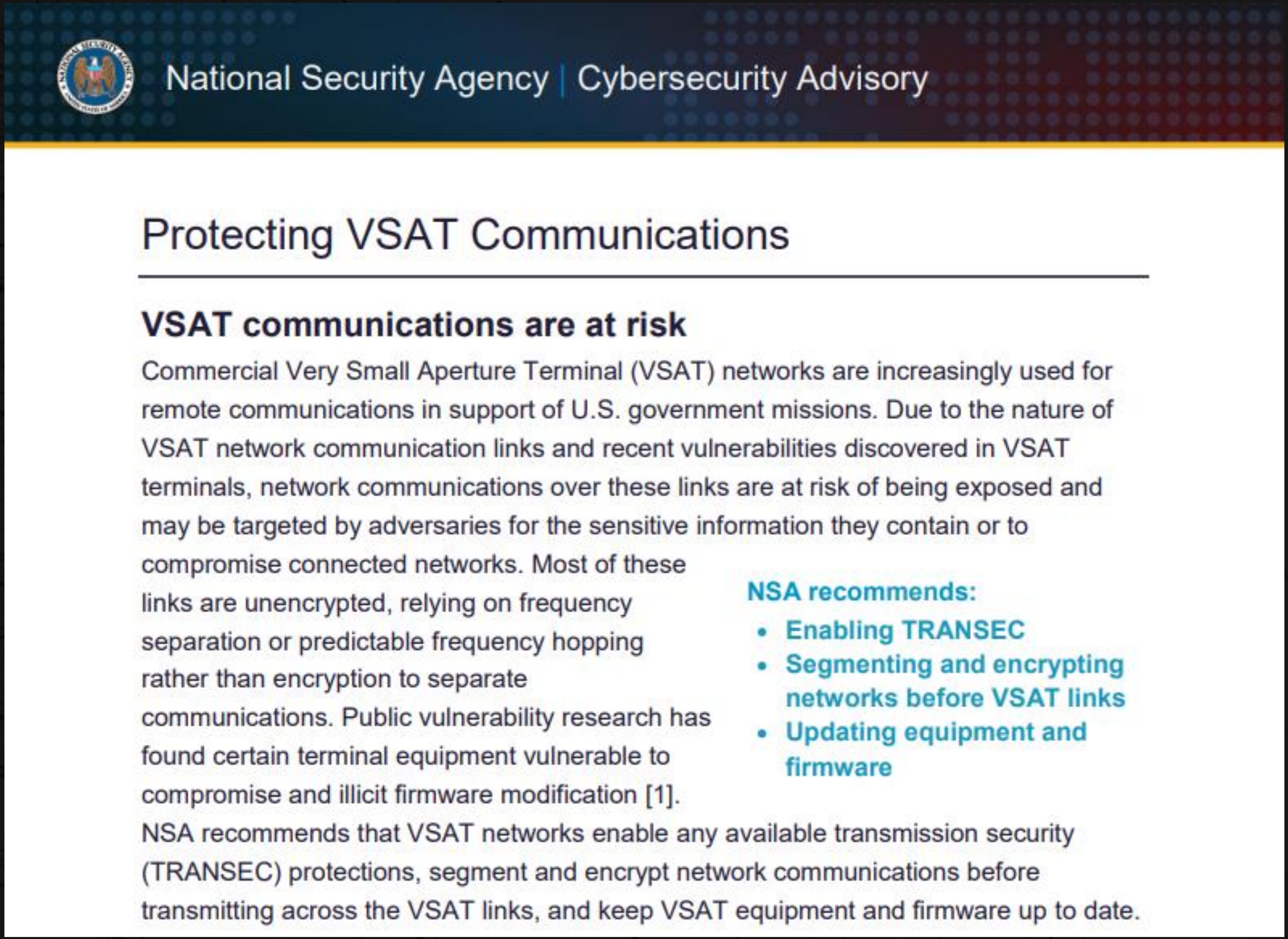
IMPACT

- Bricked at least 27,000 modems
- Affected users in Poland, Germany, UK, France, Czech Republic
- Disrupted remote monitoring and control of 5,800 wind turbines in Germany
- Impacted emergency service numbers in France for ambulance and fire services

IMPACT

- March - Victor Zhora, Deputy Chairman SSSCIP, noted that the cyber attack resulted in a “***huge loss in communications in the very beginning of the war***.”

- *“There was loss of communication, but I mean the absence of backup service. But the prime service or services [for communication], they remained operating.”* (Kim Zetter’s interview with Zhora in September)



National Security Agency | Cybersecurity Advisory

Protecting VSAT Communications

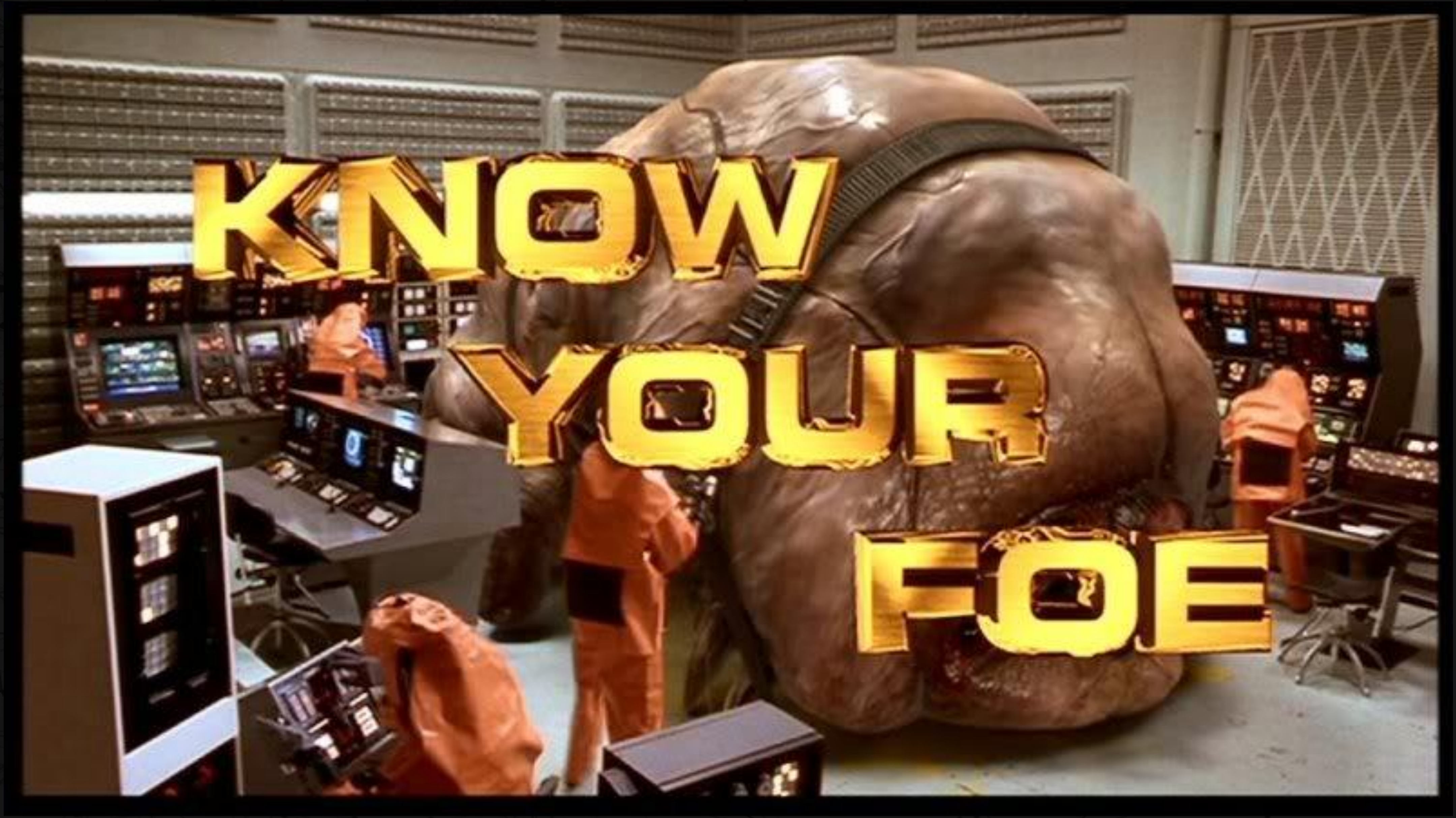
VSAT communications are at risk

Commercial Very Small Aperture Terminal (VSAT) networks are increasingly used for remote communications in support of U.S. government missions. Due to the nature of VSAT network communication links and recent vulnerabilities discovered in VSAT terminals, network communications over these links are at risk of being exposed and may be targeted by adversaries for the sensitive information they contain or to compromise connected networks. Most of these links are unencrypted, relying on frequency separation or predictable frequency hopping rather than encryption to separate communications. Public vulnerability research has found certain terminal equipment vulnerable to compromise and illicit firmware modification [1].

NSA recommends:

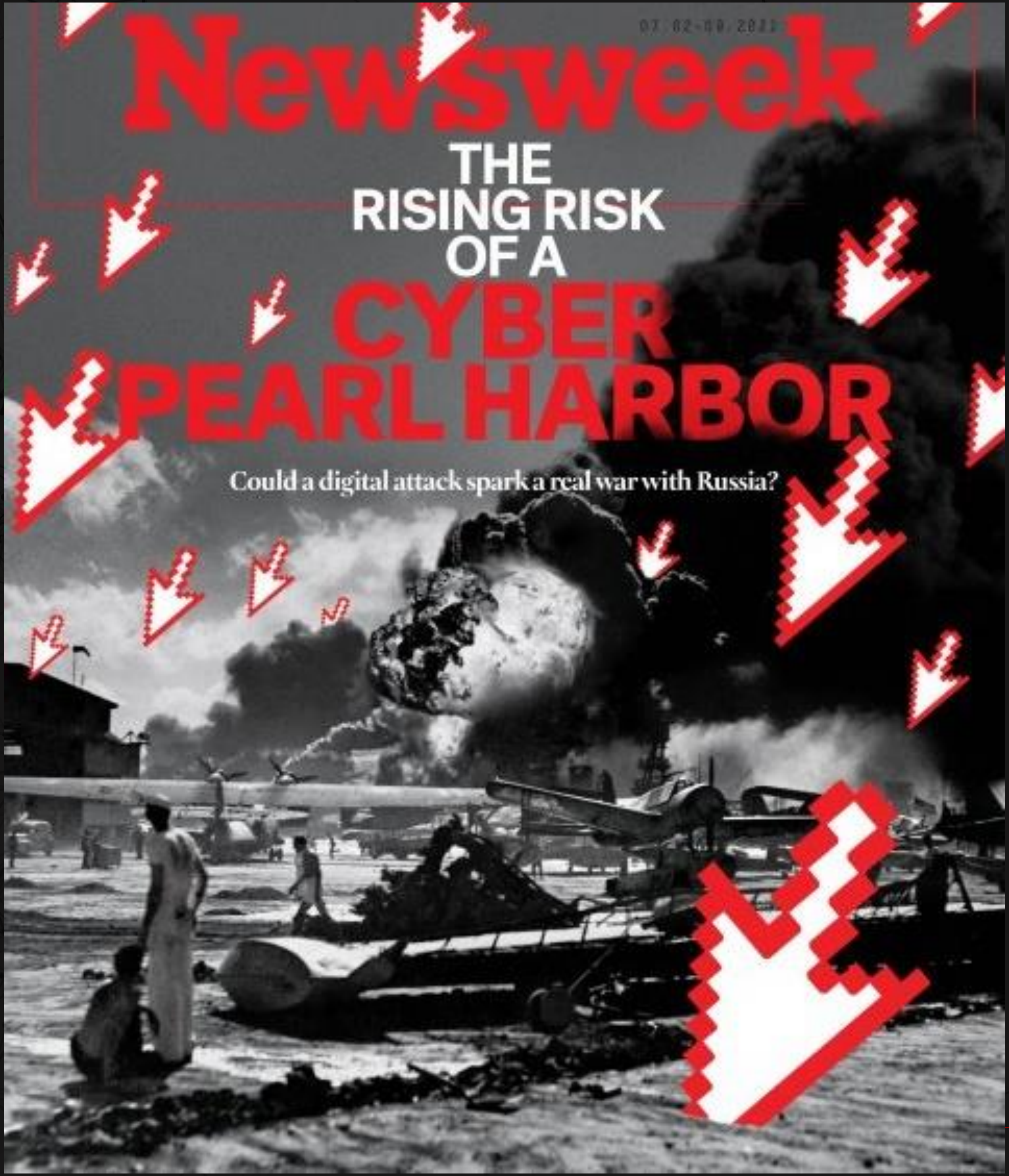
- **Enabling TRANSEC**
- **Segmenting and encrypting networks before VSAT links**
- **Updating equipment and firmware**

NSA recommends that VSAT networks enable any available transmission security (TRANSEC) protections, segment and encrypt network communications before transmitting across the VSAT links, and keep VSAT equipment and firmware up to date.


KNOW
YOUR
FOE

POINTS TO NOTE

- Cyber cyber cyberwar cyber cyber
- Space segment unaffected
- TT&C ground segment unaffected, core infra unharmed
- Cyber cyber



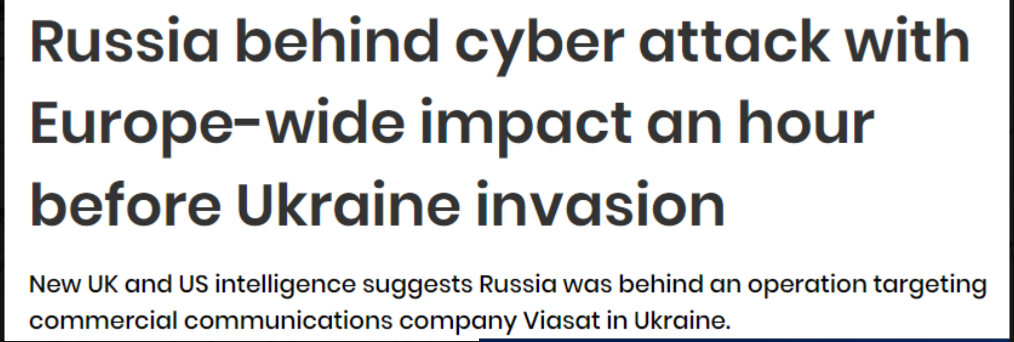
07.02-09.2021

Newsweek

THE RISING RISK OF A CYBER PEARL HARBOR

Could a digital attack spark a real war with Russia?

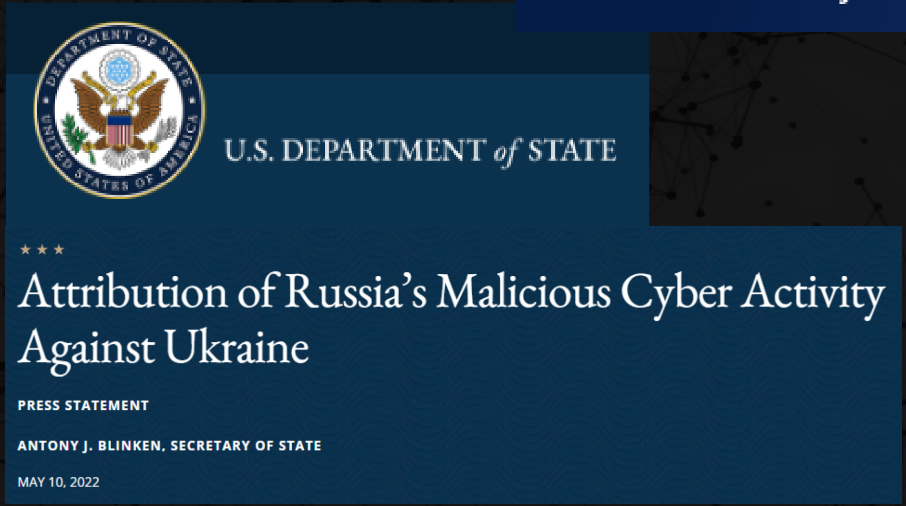
ATTRIBUTION



Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion

New UK and US intelligence suggests Russia was behind an operation targeting commercial communications company Viasat in Ukraine.

National Cyber Security Centre



U.S. DEPARTMENT *of* STATE

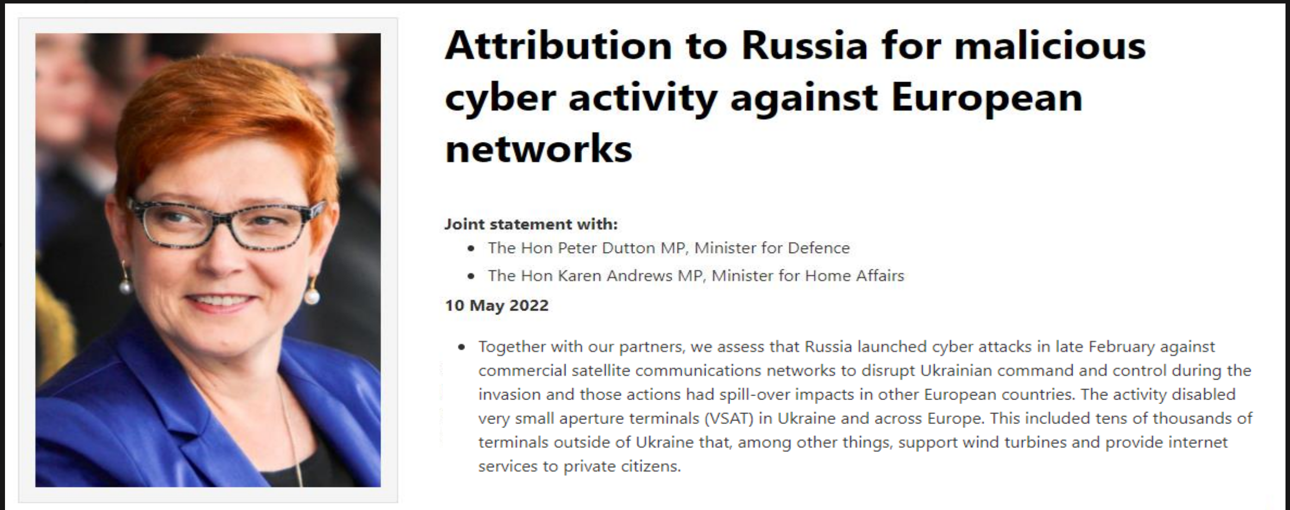
★ ★ ★

Attribution of Russia's Malicious Cyber Activity Against Ukraine

PRESS STATEMENT

ANTONY J. BLINKEN, SECRETARY OF STATE

MAY 10, 2022



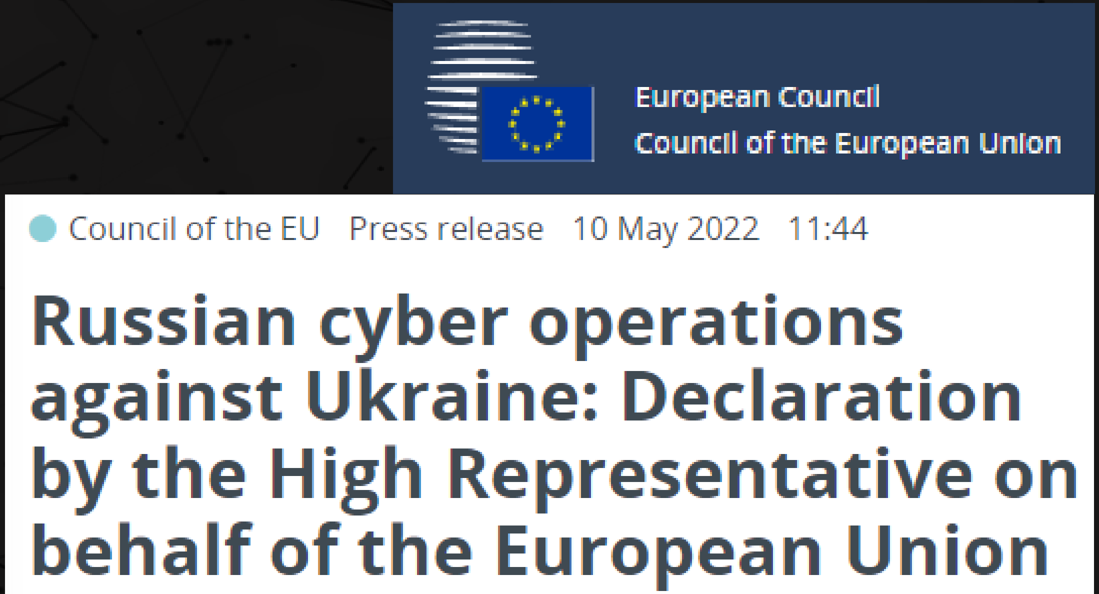
Attribution to Russia for malicious cyber activity against European networks

Joint statement with:

- The Hon Peter Dutton MP, Minister for Defence
- The Hon Karen Andrews MP, Minister for Home Affairs

10 May 2022

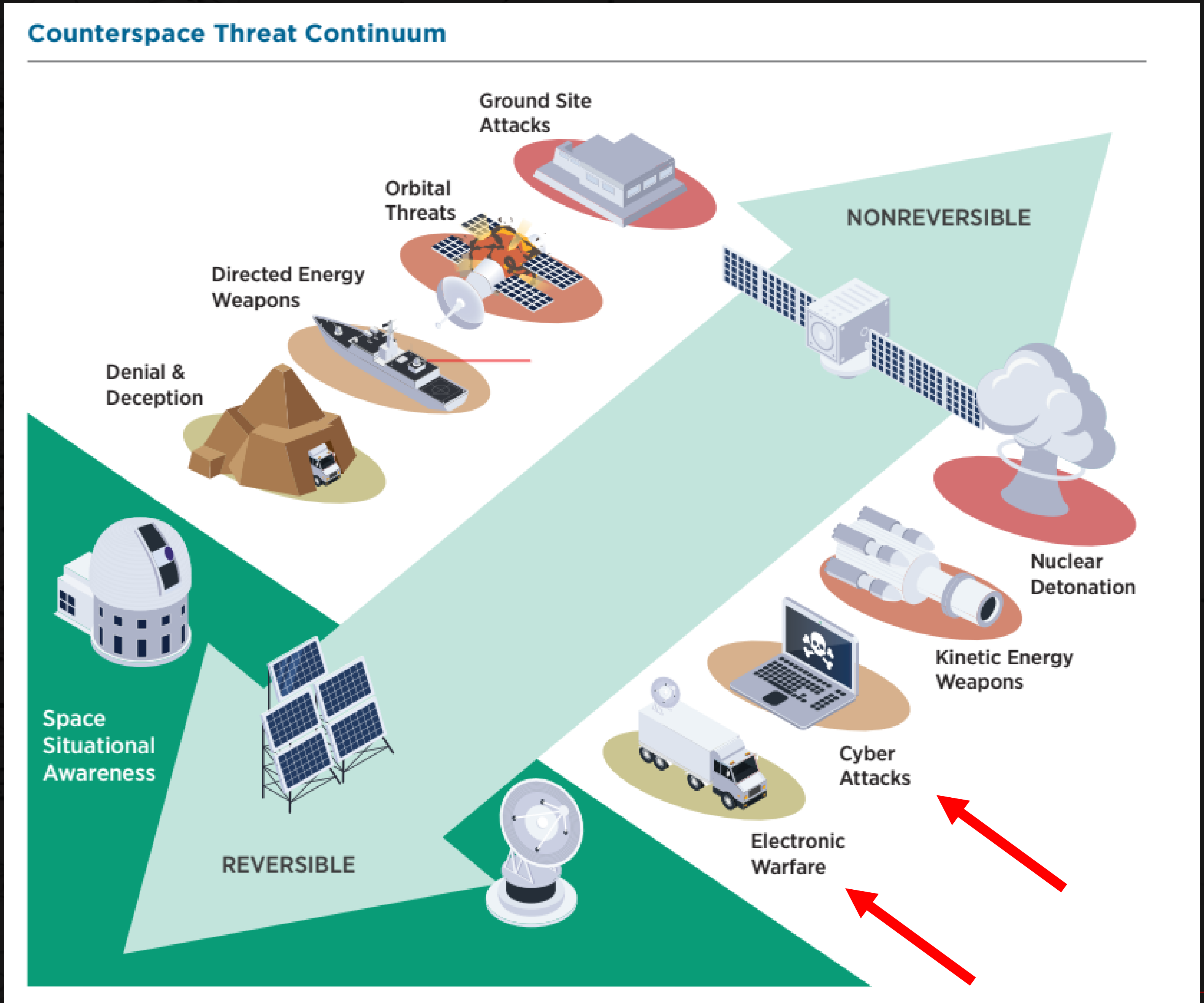
- Together with our partners, we assess that Russia launched cyber attacks in late February against commercial satellite communications networks to disrupt Ukrainian command and control during the invasion and those actions had spill-over impacts in other European countries. The activity disabled very small aperture terminals (VSAT) in Ukraine and across Europe. This included tens of thousands of terminals outside of Ukraine that, among other things, support wind turbines and provide internet services to private citizens.



European Council
Council of the European Union

Council of the EU Press release 10 May 2022 11:44

Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union



Counterspace Threat Continuum

KNOWLEDGE GAPS

- Lack of fidelity around compromise and lateral movement through management segment
- Initial compromise of modems used in DoS?
- Same or different operators?
- Intended targets

COMMAND AND CONTROL

```
[Empire]  Post-Exploitation Framework
[Version] 3.6.3 BC Security Fork | [Web] https://github.com/BC-SECURITY/Empire
[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller

      315 modules currently loaded
      0 listeners currently active
      0 agents currently active
```

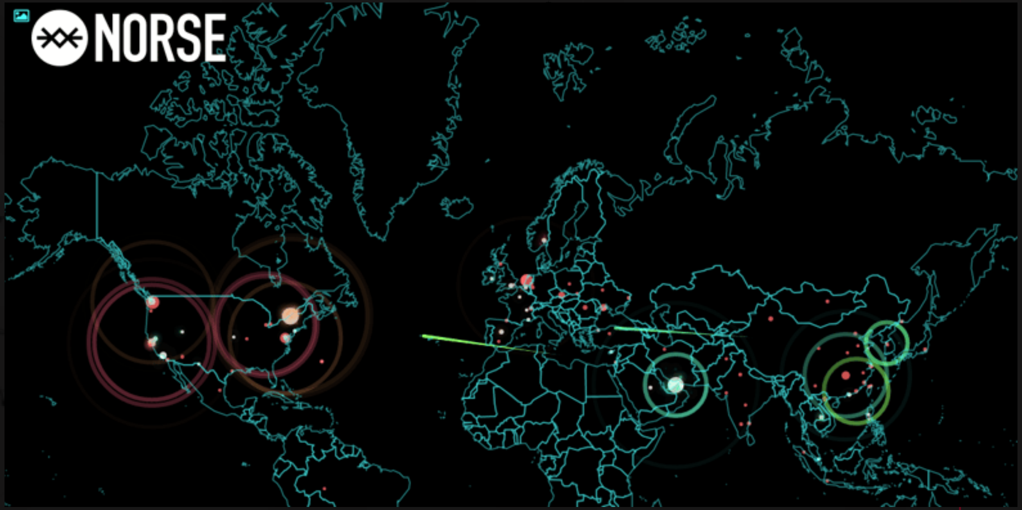
But our C2 is in another castle!

SLIVER
FRAMEWORK

- Disruption of UKR Gov/Mil C2
- Combined with RUMIL comms and GPS jamming
- Disrupting UKR CIV communications (IO/IW) – risks to shared tenancies
- Impacts to military communications minimized by pathway redundancy (PACE!)

OFFENSIVE CYBER OPERATIONS

- What systems are critical for adversary C2?
- What backup/failover systems are in place?
- How quickly can the adversary swap bearers? What impacts will swapping bearers have on participants, bandwidth, latency?
- Can EW or kinetic effects be synchronized to 4D C4 (not 4D 5A)?



How cyber attacks work, courtesy of:

KnowBe4
Human error. Conquered.

DEFENSIVE CYBER OPERATIONS

Emergency ISO27001 audits and IRAP assessments

- Maybe a low/medium DoS finding in your network isn’t that low/medium
- Detection and response measures to contain/eradicate privileged users on internal segments
- Shared bearers/infrastructure – who is co-tenanted?
- The best time to contain/eradicate the adversary was when they first compromised the network. The second best time is now.

SOURCES

- Viasat
- NATO CCDCOE
- NSA
- Kim Zetter
- SentinelOne (Juan Andres Guerrero-Saade)
- Ruben Santamara (@ReverseMode)
- WIRED
- Risky Biz
- MIT Technology Review
- Defense Intelligence Agency

THANK