

INFORMATION WARFARE AND INTEGRATED DETERRENCE

A 16TH AIR FORCE PERSPECTIVE



Lt Gen Kevin B. Kennedy
Commander



EMPOWERED AIRMEN



DELIVERING OUTCOMES



FOR THE NATION

INFORMATION

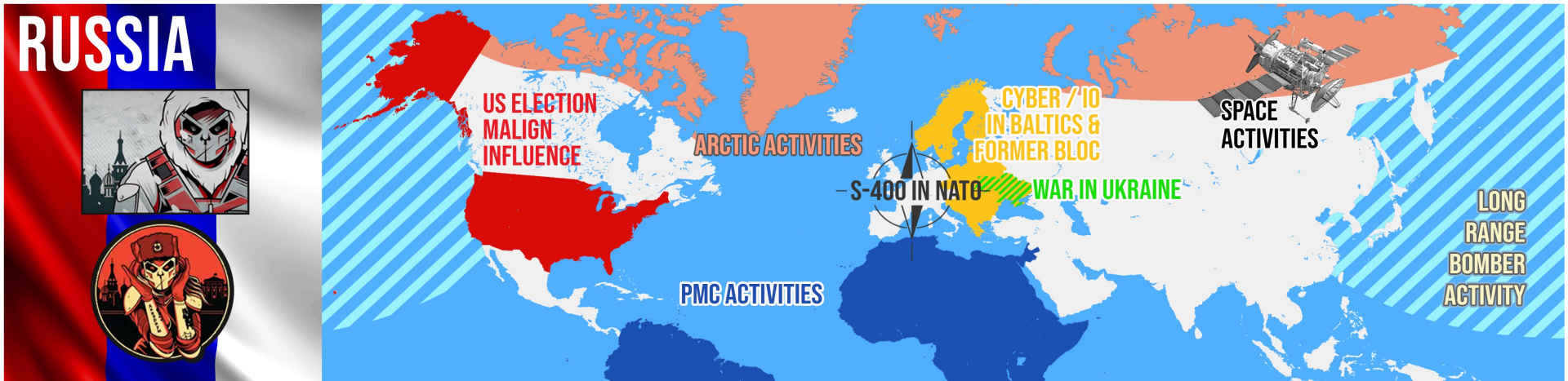
Ever-present in competition

The dominant activity in crisis

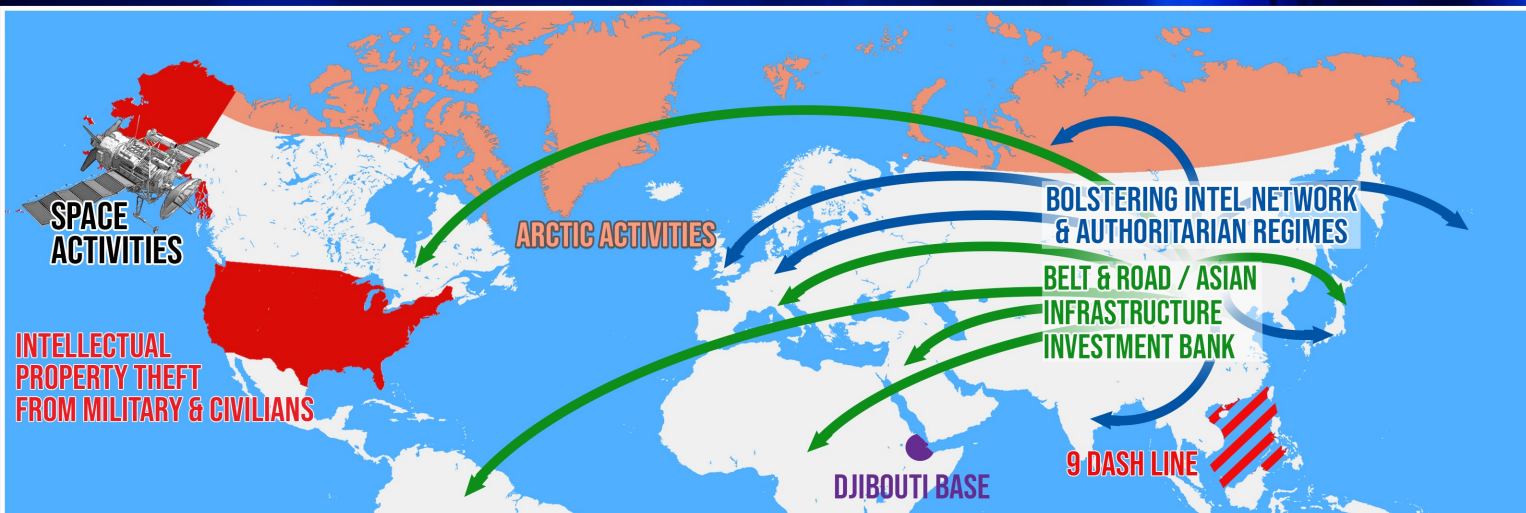
An essential enabler in conflict



WARFARE



STRATEGIC COMPETITORS CREATING ADVANTAGE





CONNECT

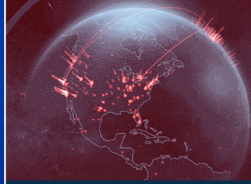


HUNT

EXPOSE



CONTEST



DEFEAT





RESILIENCE



PARTNERSHIPS



CAPABILITIES







EMPOWERED AIRMEN



DELIVERING OUTCOMES



FOR THE NATION





DAFITC 2022

A Resilient Digital
Air and Space Force:
Enabling Deterrence Through Cyber

Wendi Whitmore

Senior VP
Palo Alto Networks



Evolving Cyber Threat Landscape

A Younger Me



**YOU ARE LEAVING
THE AMERICAN SECTOR
ВЫ ВЫЕЗЖАЕТЕ ИЗ
АМЕРИКАНСКОГО СЕКТОРА
VOUS SORTEZ
DU SECTEUR AMÉRICAIN
SIE VERLASSEN DEN AMERIKANISCHEN SEKTOR**

US ARMY

Why is there no “Cyber Translate” ?

Detect Language

Expert



Beginner

Expert



Beginner

100GB of very sensitive data



Print out the data on 8x11 sheets of paper, front and back into 7 miles tall stacks. There would be about 4,700 stacks total.



Lesson 1

We have rules, they don't

THE UNFAIR ADVANTAGE

Attackers are playing a game
that we are not allowed to play.

Tales from the Trenches

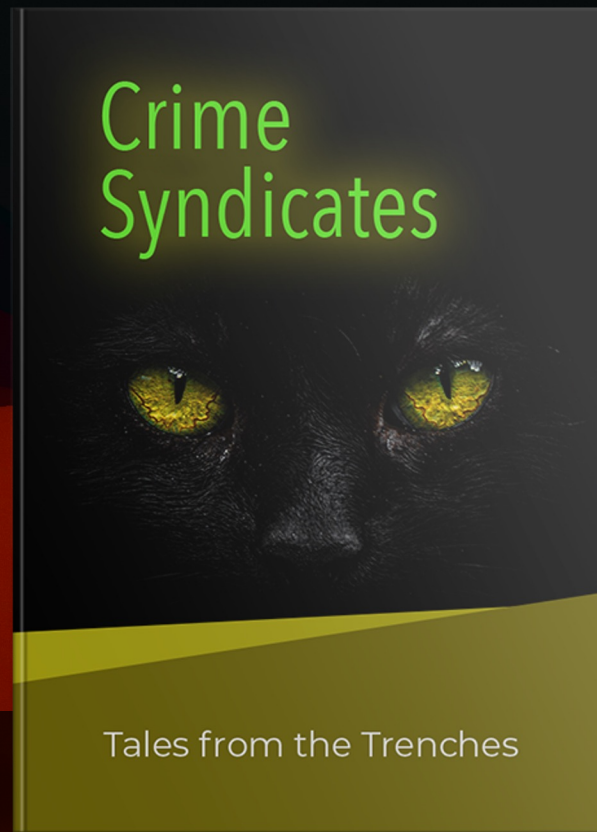
Lesson 2

It's always about money



Lesson 3

The competition is *Organized*



Lesson 4

Teamwork makes the dream work



Collaboration

to take out a Threat Actor

NOV
2021



**Victim
Attacked**

DEC
2021



**Incident
Response
Started**

JAN
2022



**Partnered
International
Agencies**

FEB
2022



**Provided
Forensics**

MAR
2022



**Partnered with
Europol; Shared
Evidence**

MAY
2022



**Incident
Response
Started
(new victims)**

Opening Negotiation

Hello and welcome to Hive. How may I help you?

Hello our files are encrypted please help.



What is the cost for the decryption software?



To decrypt your files you have to pay \$1,200,000 in Bitcoin.

Experiencing “Technical” Issues

Thank you for responding quickly. You're no mentions having our files. Can you share a file listing of the files that you have?



We don't have your files now.

What do you mean? Does that mean you never had them or you have given them to someone else?



At the moment the servers where your data resides in our unavailable.

I see. Please let us know when you restore access and are able to provide a file listing. Thank you for your help.



Do you need a detailed decryptor along with the exfiltrated files erasure?

How long will it take to establish access to the servers?



I don't know. If you pay now I guarantee that the files will be totally erased and never be disclosed anywhere.

I can give you a sufficient discount if you pay within the next few days.

What is the discount?



\$600,000

Excuses, excuses...

Are you able to provide any files to make it clear that you have our data?



Whether I'll restore an access to files I will show them to you. For you will be better to proceed without awaiting them. As I said you will get 50% discount because of this issue

Right after the access will be restored the price will also be reverted back to \$1,200,000 without any future discount.

Please, let us speak directly on the possession of data. We need to have a clear understanding on what data you have. Not that you are having trouble accessing it, which doesn't make sense, really – maybe for a day, but not for four or five days. It changes the discussion and the amount significantly.



As I said the current price for you is \$400,000 (because HDD got damaged on one of the servers wear your data resides in). If I'll be able to fix it and return back up and running the price will be reverted back. Everything is very simple now – \$400,000. I give you a promise of nondisclosure no matter the HDD status will be.

Let us agree, you do not have our data therefore cannot and will not publish anything publicly. Yes? With that out-of-the-way, let us focus only on the value/price of the description software. Yes or No?



Final Offer!

Thank you for responding. Please, we need an amount under \$100,000.



No, \$200,000 is the final price for you

As we mentioned, the amount needs to be under \$100,000. The reason is the board will have to approve any payment and we cannot go to them with any proposal that is higher. Please strongly consider this lower amount. Thank you.



OK, it will be a present for past holidays \$100,000

Outcomes that Change the Game

- Prevented Financial Loss
- Prevented Sensitive Data Leakage
- Denied Threat Actor Ransom Funds
- Damaged Threat Actor's Reputation
- Provided valuable info to Law Enforcement

\$1.2M



\$100k

Connect with me

[linkedin.com/in/wendiwhitmore](https://www.linkedin.com/in/wendiwhitmore)

2
@wendiwhitmor
e

Q&A

Connect with me

linkedin.com/in/wendiwhitmore

2
@wendiwhitmor
e