Cyber War is Boring

@LegendaryPatMan

paddy@cyberwarfa.re

Who Am I?

Digital Forensics and Cyber Security Graduate from TU Dublin

Community Manager for the Arms Control Wonk network of blogs and podcasts where I;

Plan needs and attempt to implement solutions
Do OSINT and sometimes get in the Economist or the WaPo
Research Information Warfare

Sources: Blog post tbd but the link shows all IW posts

https://blog.cyberwarfa.re/tag/iw-cw/

https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information
https://twitter.com/DDaltonBennett/status/1238113640563249155?s=20
https://www.armscontrolwonk.com/archive/1208771/investigating-ps752-with-open-source-intelligence/

Disclaimer

Discussion of the War in Ukraine to follow

Possible PTSD Triggers due to imagery and audio of equipment being damaged and destroyed

“So far, I'm hearing lots of concern about the possibility of massive cyber attacks, but very little evidence of any such thing”

Don Edwards

https://discord.com/channels/798533956466901012/935571191933075518/946460463502356530

War Is Boring

"… *that much of warfare is about politics, paperwork and logistics more than it is about actual combat.*"

David Axe

https://smallwarsjournal.com/author/war-is-boring

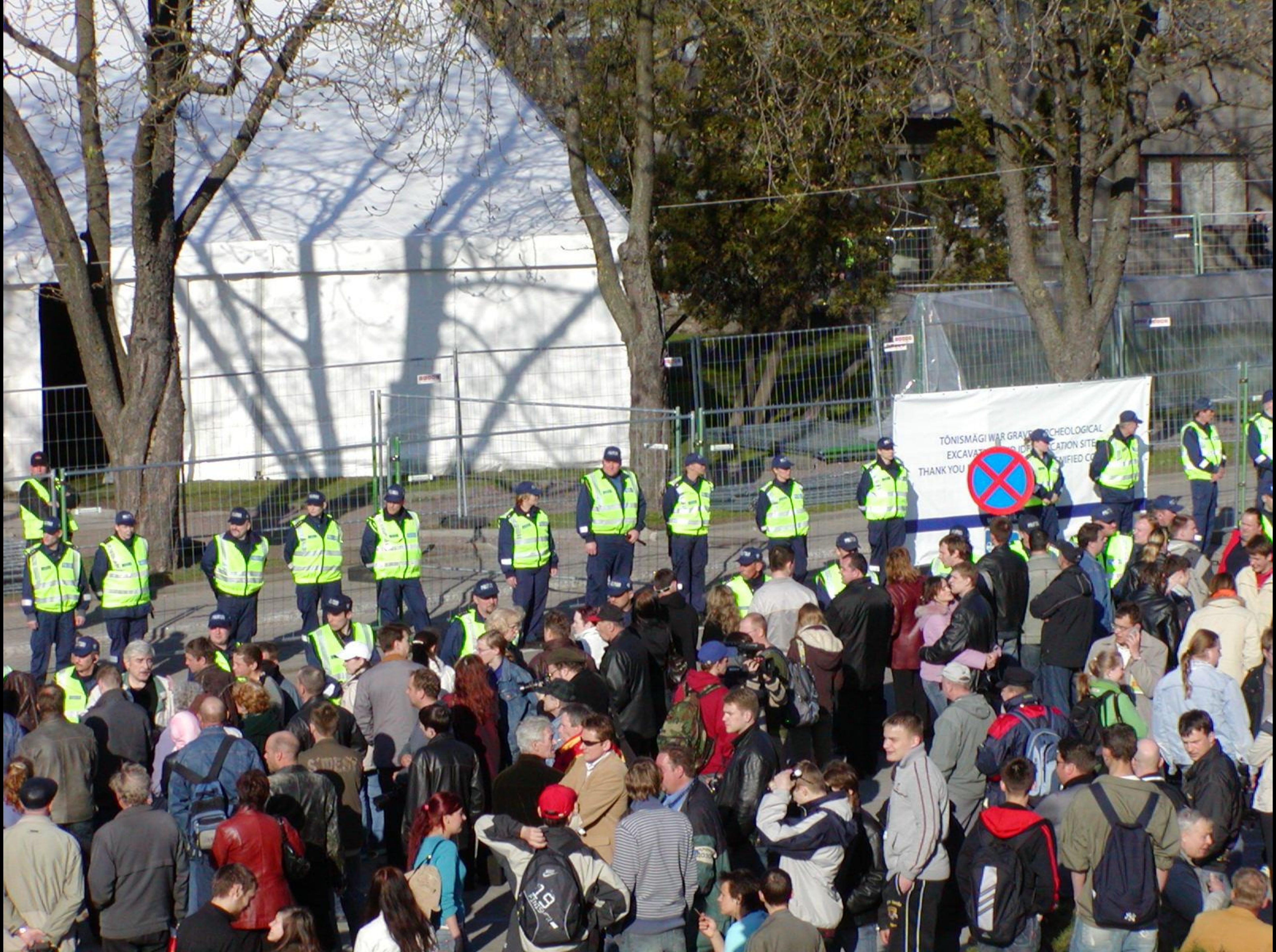
Politics

"*Cyber war is an extension of policy by actions taken in cyber space by state or nonstate actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security.*"

Paulo Shakarian, Jana Shakarian and Andrew Ruef

Introduction to Cyber-Warfare - A Multidisciplinary Approach, pp 2

ОТЕЧЕСТВЕННАЯ ВОЙНА
TEISES
MAAILMASÕJAS
HUKKUNUTELE
ПАВШИМ
ВО ВТОРОЙ
МИРОВОЙ ВОЙНЕ


TÕNISMÄGI WAR GRAV RCHEOLOGICAL
EXCAVAT   D IDE   CATION SITE
THANK YOU   NIFIED CO

"KOSMOS"

Hybrid Warfare

Strategically aimed Political Warfare against Democracies and Democratic intuitions that blending conventional warfare;

Russian backed "*Uprisings* " in the Donbass and Lunhansk

Irregular Warfare

Little Green Men in Crimea 2014

Cyber Warfare

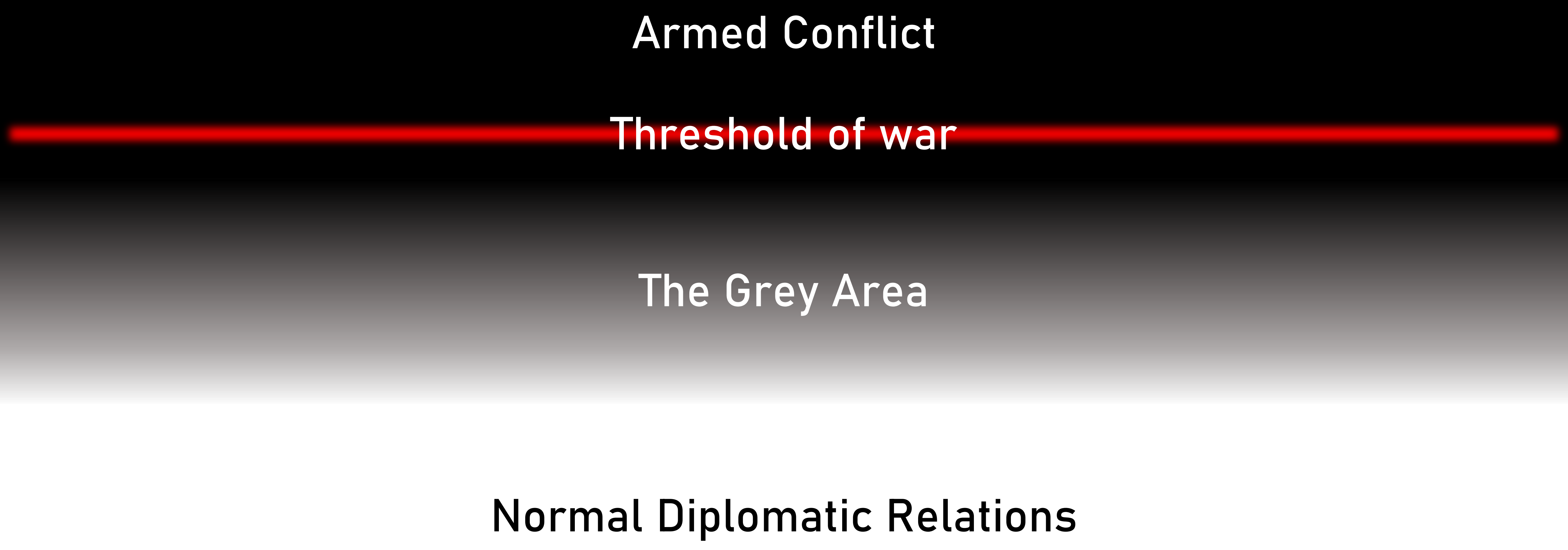
The Bears/GhostWriter defacing sites, Ukraine 2022

Influence Operations

Disinformation, Propaganda, Active Measures

https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Grey Area Operations



Armed Conflict

Threshold of war

The Grey Area

Normal Diplomatic Relations

Legalities

“…*there is no known cyber attack that unequivocally meets Clausewitz’s first criterion: violence. No cyber offense has ever caused the loss of human life. No cyber offense has ever injured a person. No cyber attack has ever damaged a building.*”

Thomas Rid

https://doi.org/10.1080%2F01402390.2011.608939

Criminal Justice (Offences Relating to Information Systems) Act 2017

"An Act to give effect to certain provisions of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA; for those and other purposes to amend the Criminal Damage Act 1991, the Bail Act 1997 and the Criminal Justice Act 2011; and to provide for related matters."

Tithe an Oireachtas

https://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/print.html

Cyber Attacks are an internationally defined legal concept, whereby a Cyber Operation [1] is carried out by a Subject of International Law that is reasonably expected to cause injury or death to persons or damage or destruction to objects [2] [3].

A Cyber Operation is the use of cyber capabilities to totally or partially destroy, capture, or neutralize tangible objects such as computers, networks, and other infrastructure in cyberspace, which make an effective contribution to military action by their nature, location, purpose, or use [4]. This effort is made to link the attacks to existing Humanitarian Law, but also because existing law expects that the use of such a capability should have the same impacts and characteristics as a kinetic weapon [5]. This Cyber Operation must also be carried out by someone subject to international law as not everyone is, these people are called Subjects of International Law. Subjects are limited to States, Entities Legally Proximate to States, Entities Recognized as Belligerents, International Administration of Territories Prior to Independence, and International Organizations [4]. Beyond this, Individuals, Corporations, Non-Self-Governing Peoples, and Entities Sui Generis in specific situations, such as Human Rights, Trade Law, National Liberation Movements, and the Roman Catholic Church respectively [6].

The criteria one should be looking for to identify a cyber intrusion as a Cyber Attack is;

❔ Was there a Cyber Operation?
❔ Was such an intrusion reasonably expected to cause injury or death to persons or damage or destruction to objects?
❔ Was the intrusion carried out by an actor Subject to International Law

1. Schmitt, et al, 2018. Tallinn Manual 2.0. On the International Law Applicable to Cyber Operations. 1st ed. Cambridge: Cambridge University Press, pp.521.
2. Schmitt, M., 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare. 1st ed. Cambridge: Cambridge University Press, pp.106-110.
3. Schmitt, et al, 2018. Tallinn Manual 2.0. On the International Law Applicable to Cyber Operations. 1st ed. Cambridge: Cambridge University Press, pp.415-420.
4. Schmitt, et al, 2018. Tallinn Manual 2.0. On the International Law Applicable to Cyber Operations. 1st ed. Cambridge: Cambridge University Press, pp.435-445.
5. Brown, G. and Metcalf, A., 2014. Easier Said Than Done: Legal Reviews of Cyber Weapons. Journal of National Security Law & Policy, Vol 7(No 1).
6. Crawford, J. R., 2012. Brownlie's Principles of Public International Law. 8th ed. Oxford: Oxford University Press, pp.115-126.

The Important Bit on Cyber Attacks

The criteria one should be looking for to identify a cyber intrusion as a Cyber Attack is;

Was there a Cyber Operation?

Was such an intrusion reasonably expected to cause injury or death to persons or damage or destruction to objects i.e. was there Violence ?

Was the intrusion carried out by an actor Subject to International Law ?

Cyber War Will Not Take Place

"Cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future. Instead, all past and present political cyber attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage. That is improbable to change in the years ahead."

Thomas Rid

https://doi.org/10.1080%2F01402390.2011.608939

The Subversive Trilemma

"…we thus should not confuse what is theoretically possible with what is practically feasible."

Effective Cyber is limited by;

Operational speed;

Effective + secret recon, exploit dev and exploit use takes time as does learning systems/networks post exploit

Intensity of effects;

Big effects require a lot of action - or control - and noise gives up the game

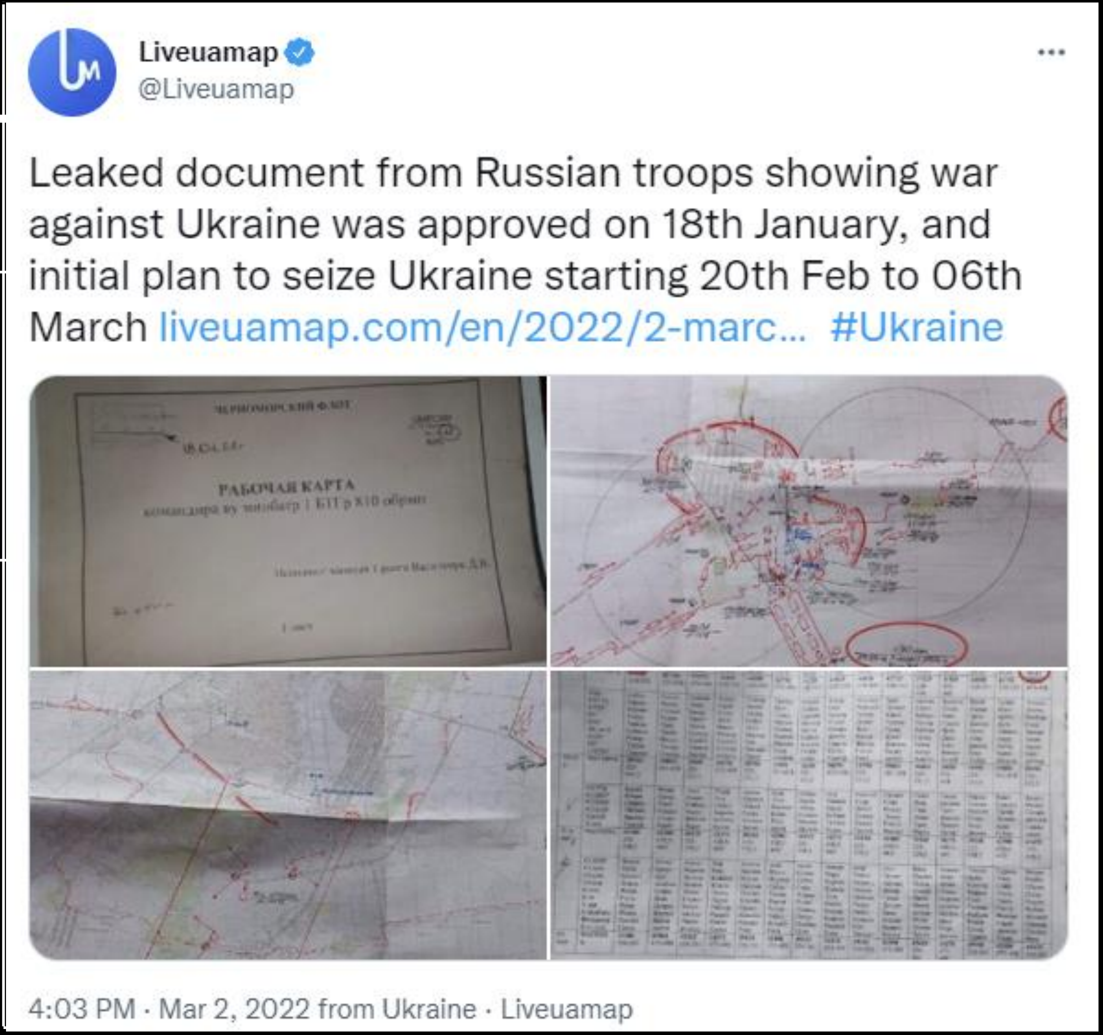
System control;

Avoiding detection requires minimal system control

https://direct.mit.edu/isec/article/46/2/51/107693/The-Subversive-Trilemma-Why-Cyber-Operations-Fall

The Subversive Trilemma

	Stuxnet
Speed	5 year dev + 1Bn USD
Intensity	Possible Equipment destruction? Slowed nuclear program
Control	0.500 had no C2, was secret - zero control 1.001 had C2 but control was lost when it spread globally



Liveuamap
@Liveuamap

Leaked document from Russian troops showing war against Ukraine was approved on 18th January, and initial plan to seize Ukraine starting 20th Feb to 06th March liveuamap.com/en/2022/2-marc... #Ukraine

4:03 PM · Mar 2, 2022 from Ukraine · Liveuamap

Perceptions

“… it’s not the cyber war we were promised.”

Adam Boileau

https://www.risky.biz/RB652/ @ 05:10

780

"STREN

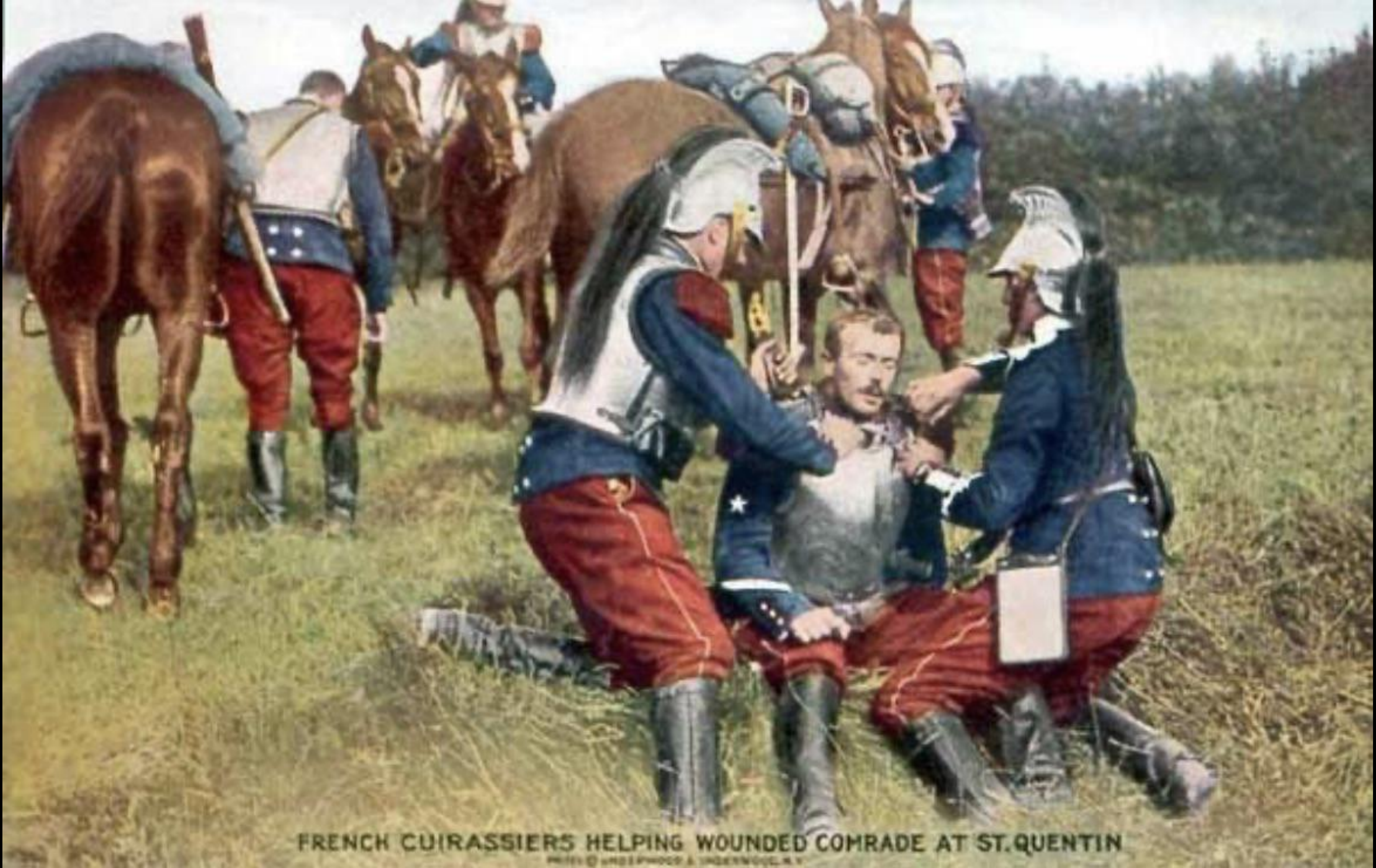
96

S. Caceres
PHOTOGRAPHY

Every age has its own kind of war, its own limiting conditions, and its own peculiar preconceptions.

Carl von Clausewitz

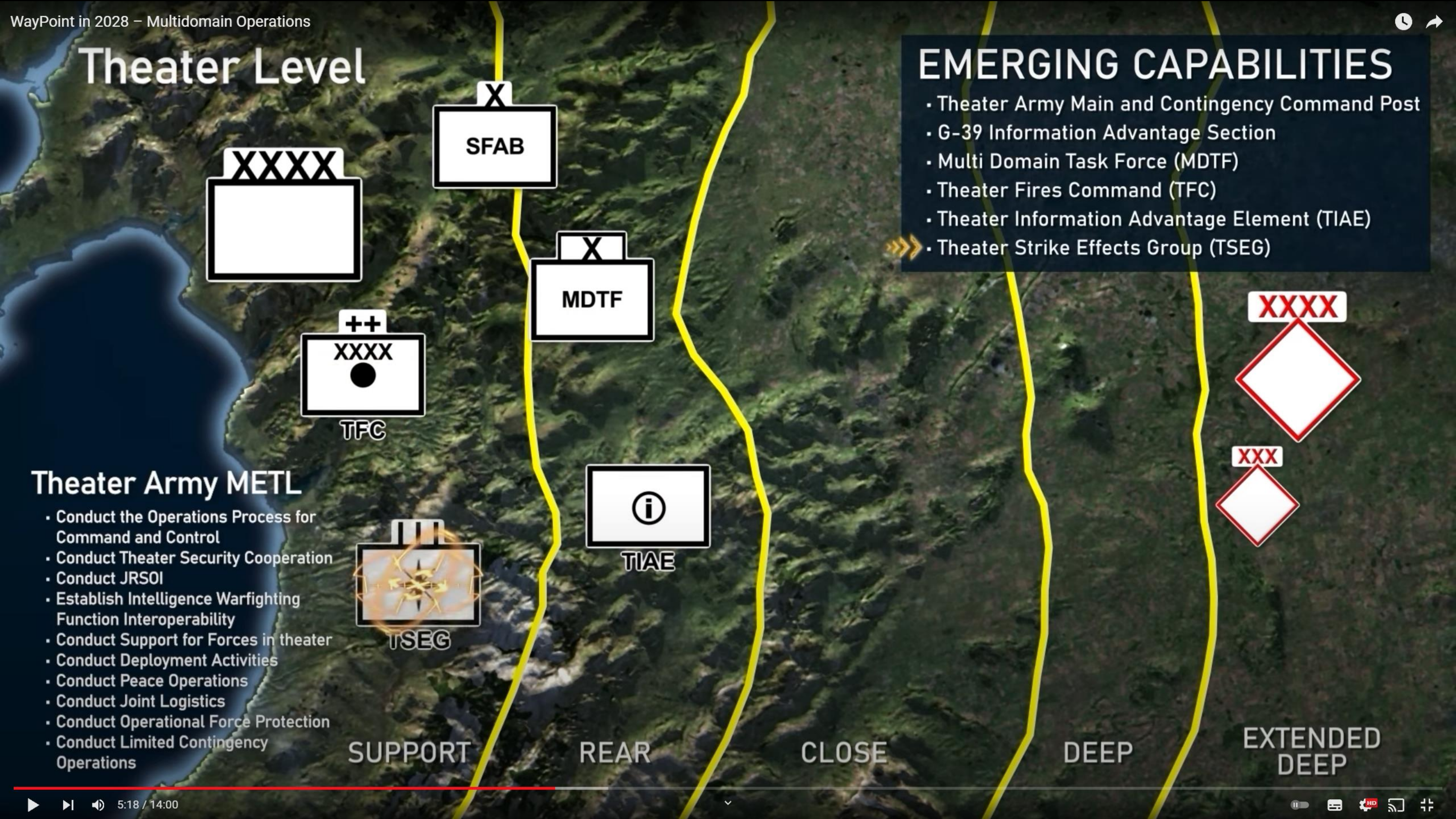
On War, pp 593



FRENCH CUIRASSIERS HELPING WOUNDED COMRADE AT ST. QUENTIN

PHOTO © UNDERWOOD & UNDERWOOD, N.Y.

© Images University of Aberdeen



WayPoint in 2028 – Multidomain Operations

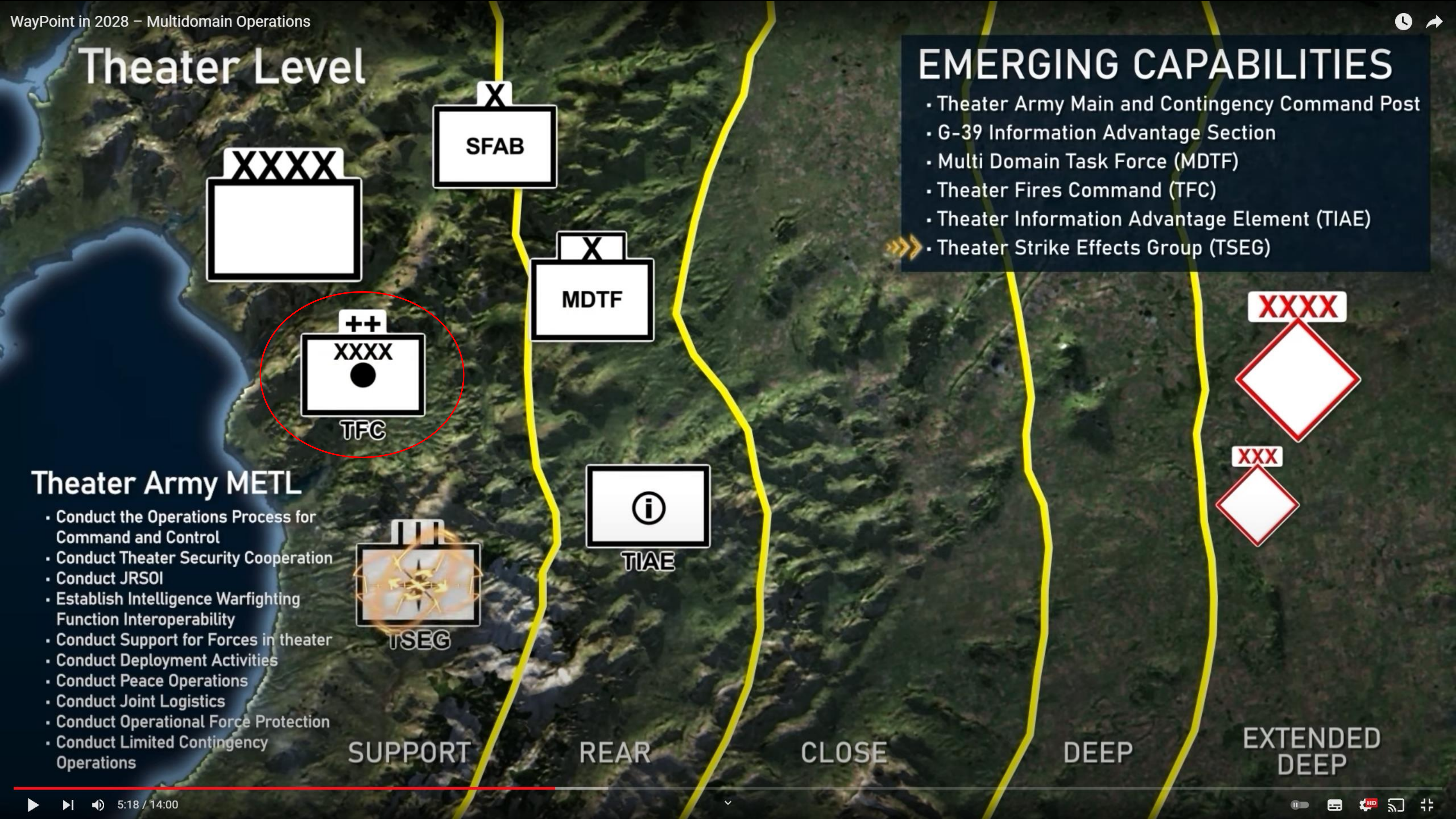
Theater Level

EMERGING CAPABILITIES

- Theater Army Main and Contingency Command Post
- G-39 Information Advantage Section
- Multi Domain Task Force (MDTF)
- Theater Fires Command (TFC)
- Theater Information Advantage Element (TIAE)
- Theater Strike Effects Group (TSEG)

Theater Army METL

- Conduct the Operations Process for Command and Control
- Conduct Theater Security Cooperation
- Conduct JRSOI
- Establish Intelligence Warfighting Function Interoperability
- Conduct Support for Forces in theater
- Conduct Deployment Activities
- Conduct Peace Operations
- Conduct Joint Logistics
- Conduct Operational Force Protection
- Conduct Limited Contingency Operations



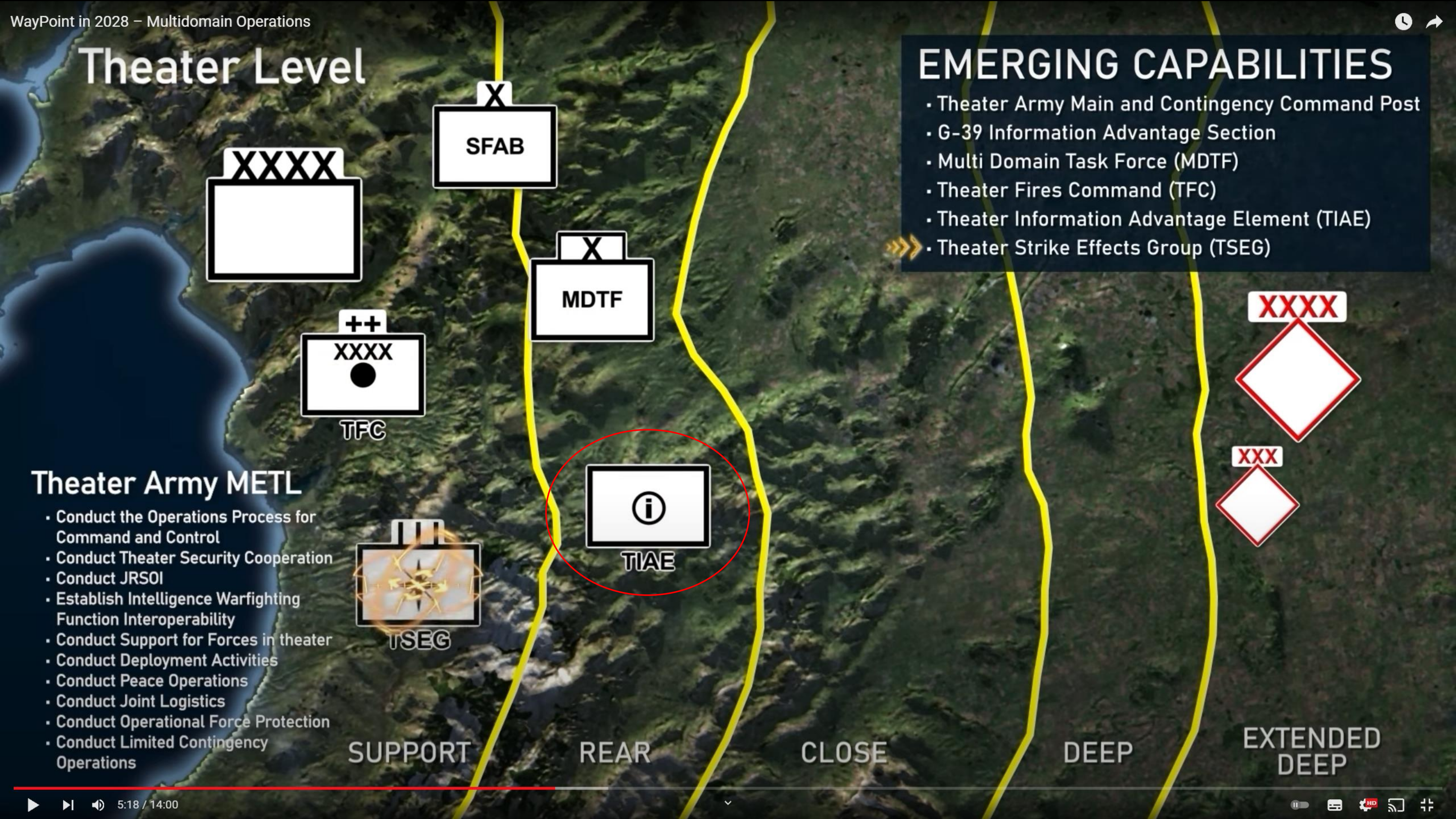
Theater Level

EMERGING CAPABILITIES

- Theater Army Main and Contingency Command Post
- G-39 Information Advantage Section
- Multi Domain Task Force (MDTF)
- Theater Fires Command (TFC)
- Theater Information Advantage Element (TIAE)
- Theater Strike Effects Group (TSEG)

Theater Army METL

- Conduct the Operations Process for Command and Control
- Conduct Theater Security Cooperation
- Conduct JRSOI
- Establish Intelligence Warfighting Function Interoperability
- Conduct Support for Forces in theater
- Conduct Deployment Activities
- Conduct Peace Operations
- Conduct Joint Logistics
- Conduct Operational Force Protection
- Conduct Limited Contingency Operations



WayPoint in 2028 – Multidomain Operations

Theater Level

EMERGING CAPABILITIES

- Theater Army Main and Contingency Command Post
- G-39 Information Advantage Section
- Multi Domain Task Force (MDTF)
- Theater Fires Command (TFC)
- Theater Information Advantage Element (TIAE)
- Theater Strike Effects Group (TSEG)

Theater Army METL

- Conduct the Operations Process for Command and Control
- Conduct Theater Security Cooperation
- Conduct JRSOI
- Establish Intelligence Warfighting Function Interoperability
- Conduct Support for Forces in theater
- Conduct Deployment Activities
- Conduct Peace Operations
- Conduct Joint Logistics
- Conduct Operational Force Protection
- Conduct Limited Contingency Operations

2018 US DoD Cyber Strategy

Persistent Engagement

Everywhere and Always… In the fight

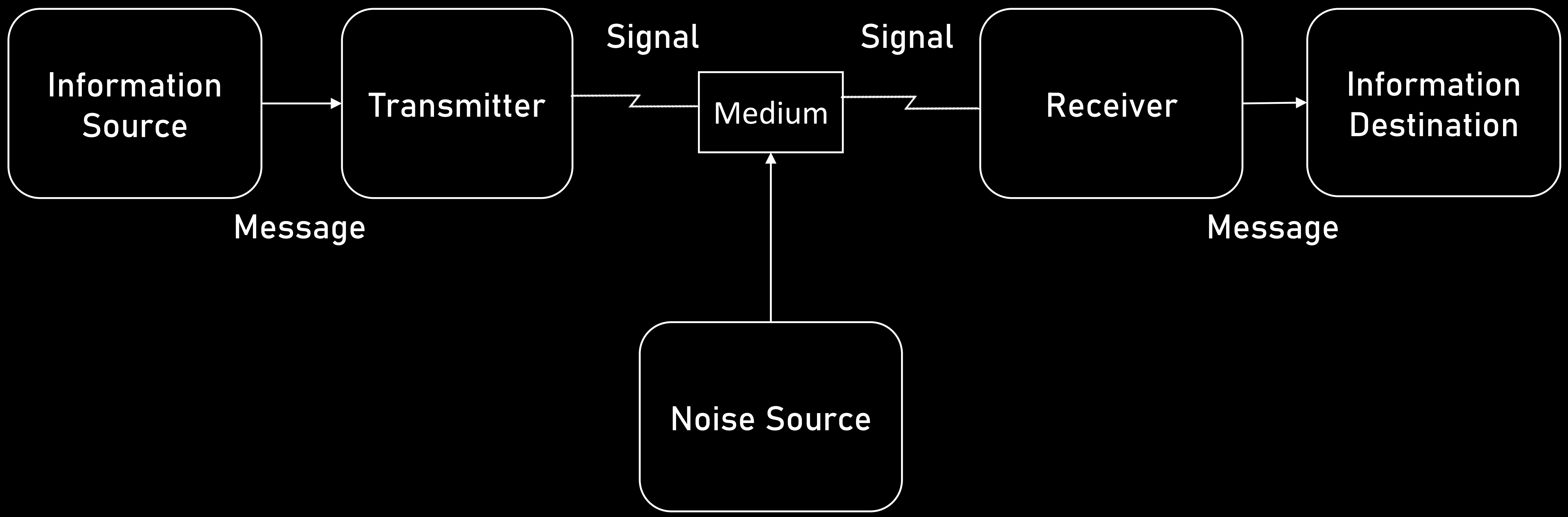
Defend Forward

Counter adversary “at their source”

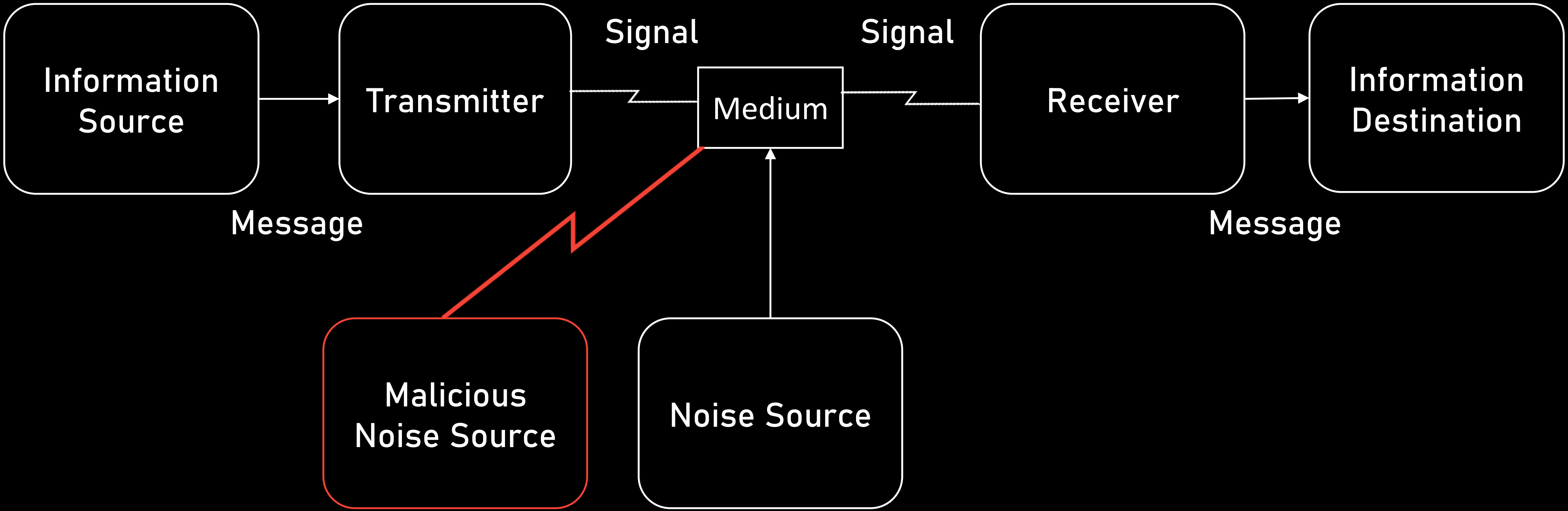
Protect friendly information – OPSEC
inform and influence activities - impact adversary decision making while making sure commanders can make thee right call

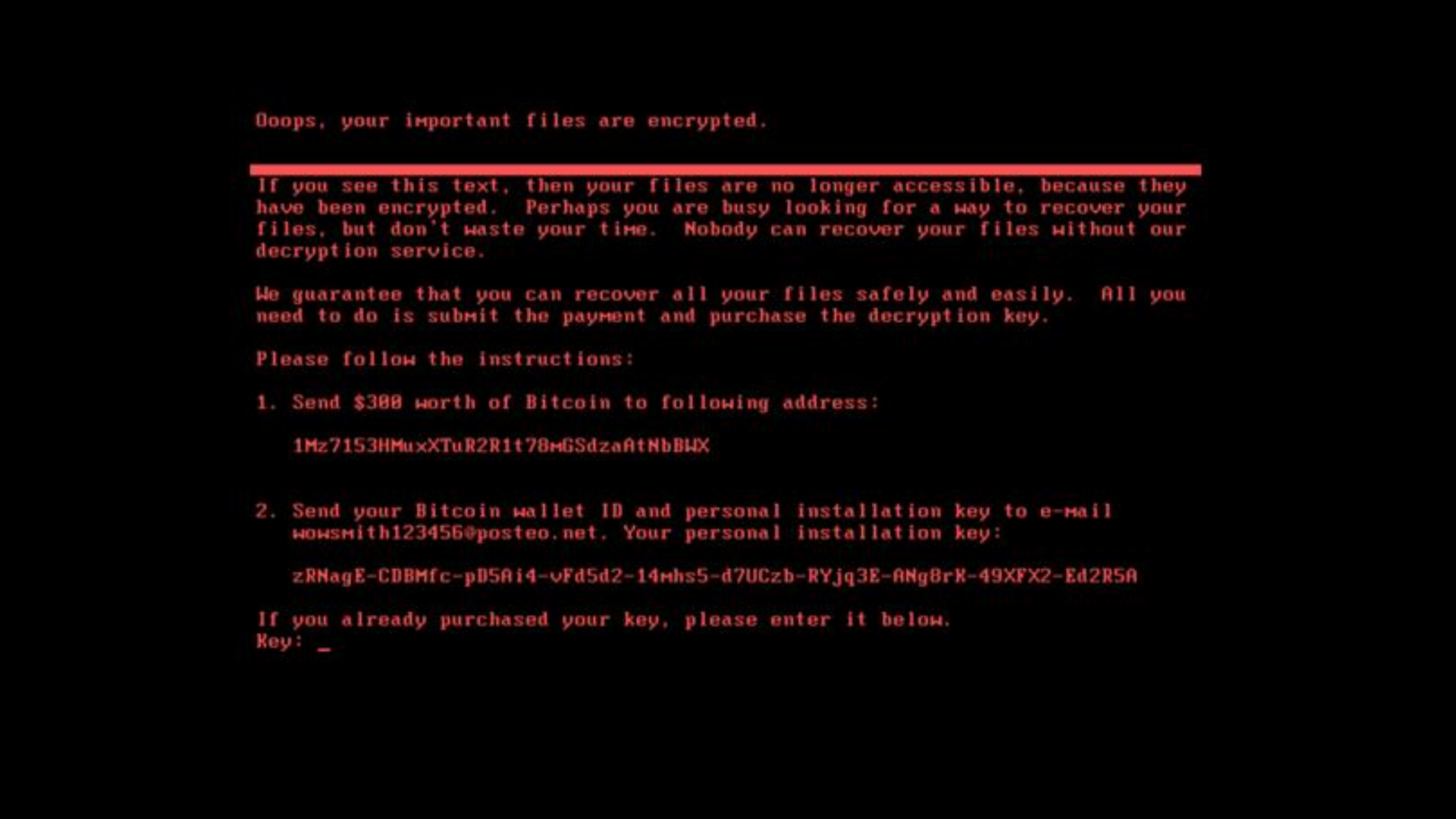
https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy
https://youtu.be/OUZp01Cjdil

Limitations

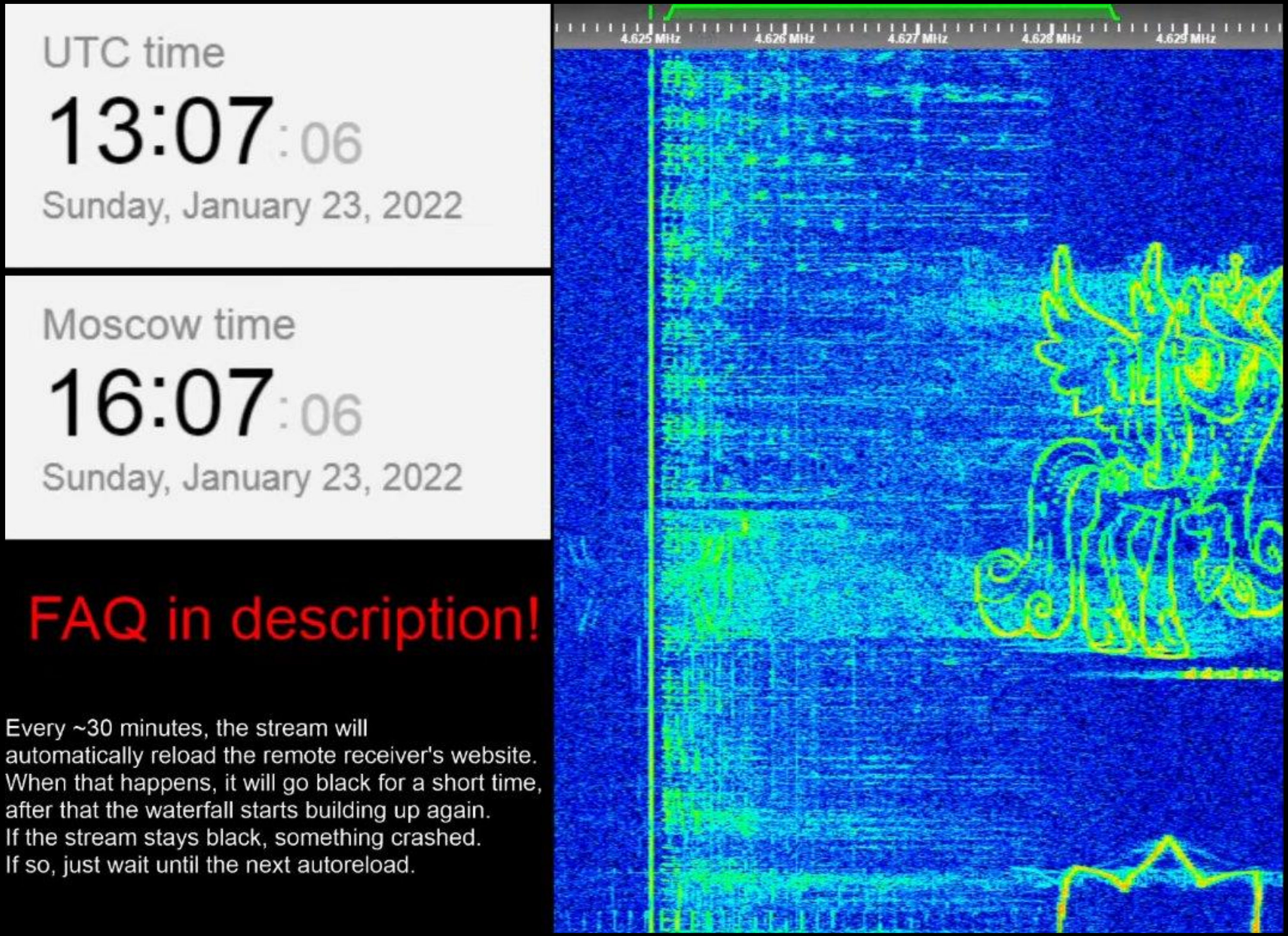


Attacks that Degrade Information





```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```



UTC time

13:07:06

Sunday, January 23, 2022

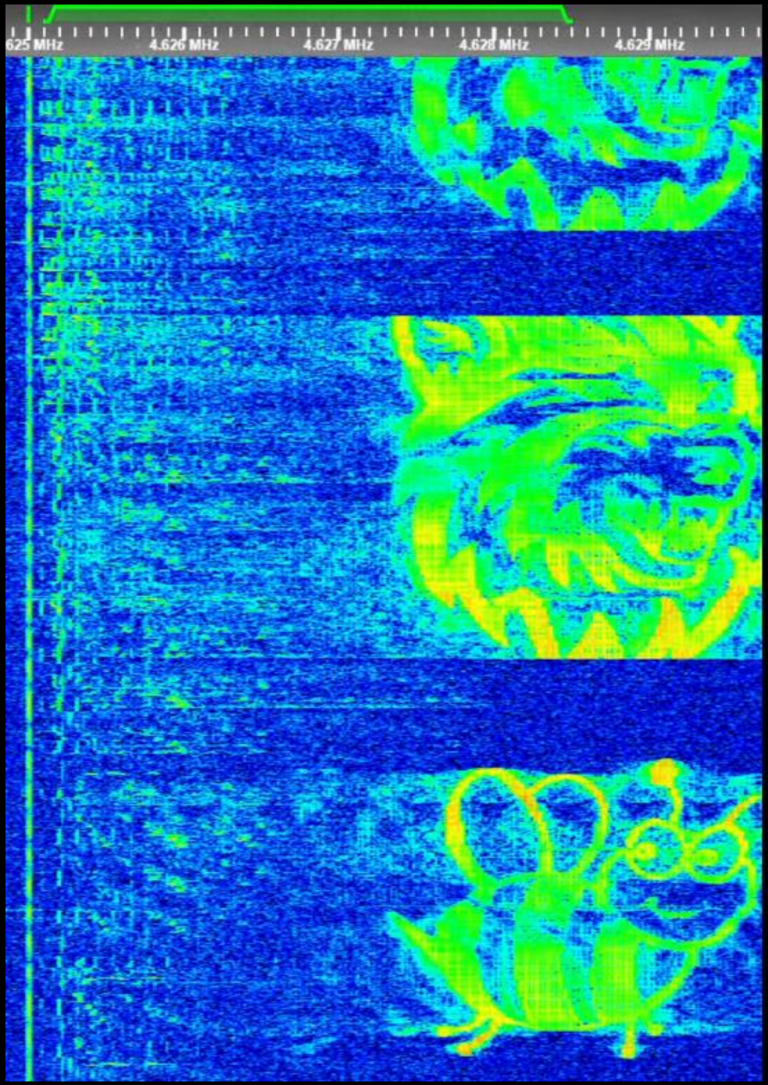
Moscow time

16:07:06

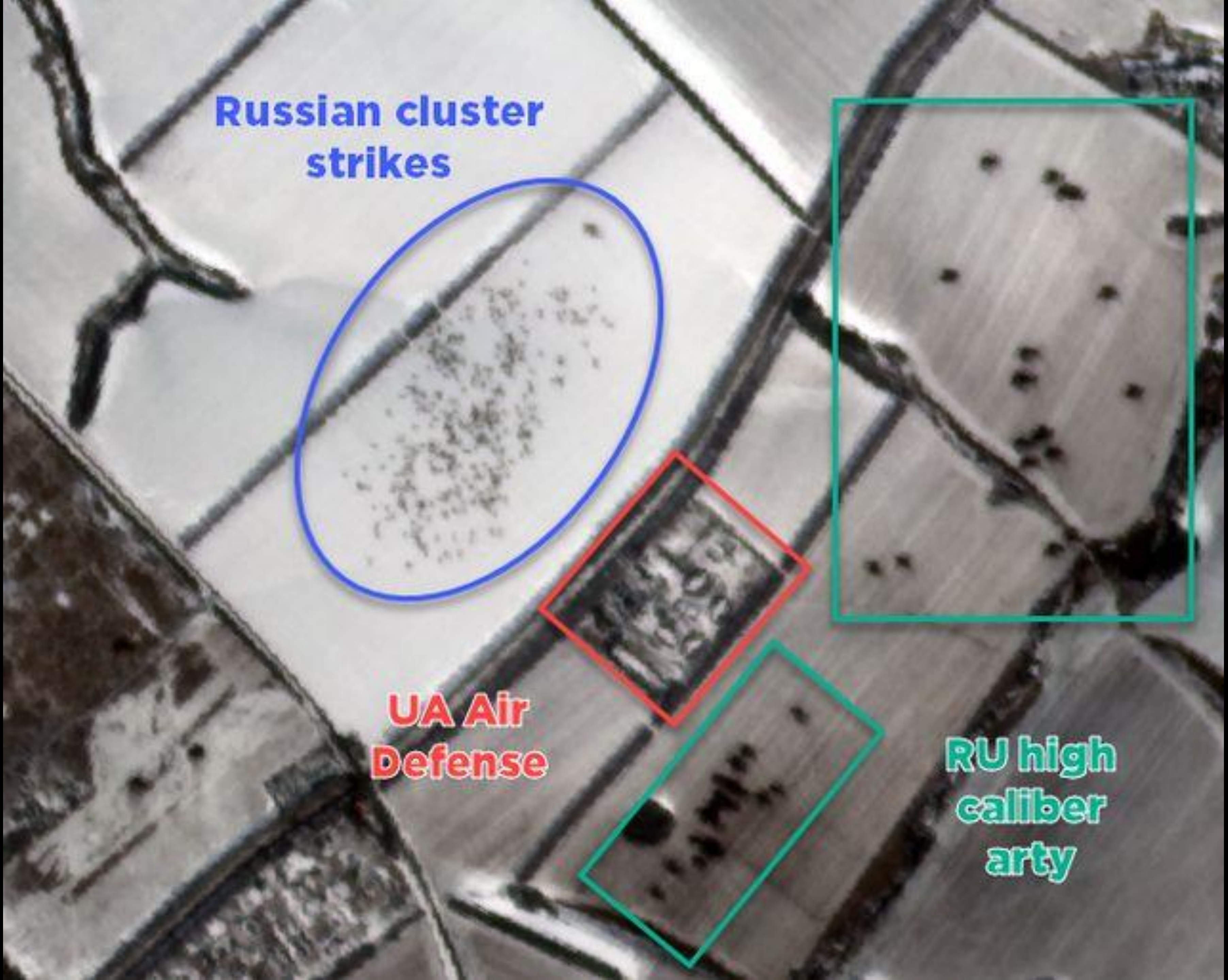
Sunday, January 23, 2022

FAQ in description!

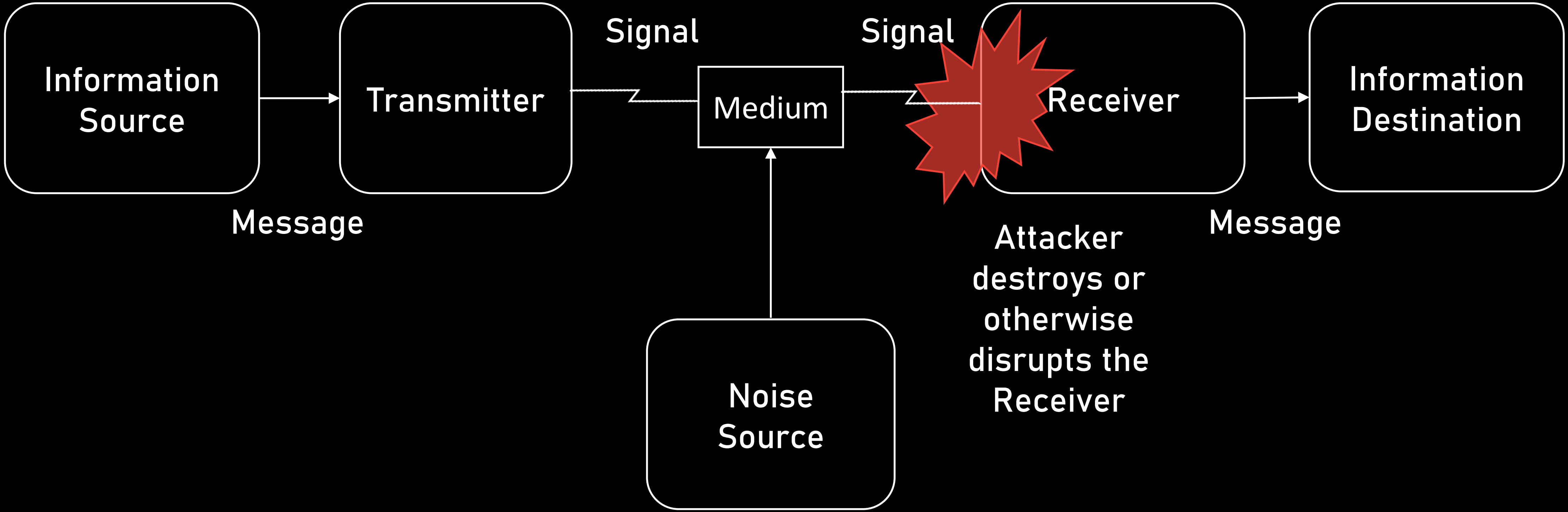
Every ~30 minutes, the stream will automatically reload the remote receiver's website. When that happens, it will go black for a short time, after that the waterfall starts building up again.
If the stream stays black, something crashed.
If so, just wait until the next autoreload.



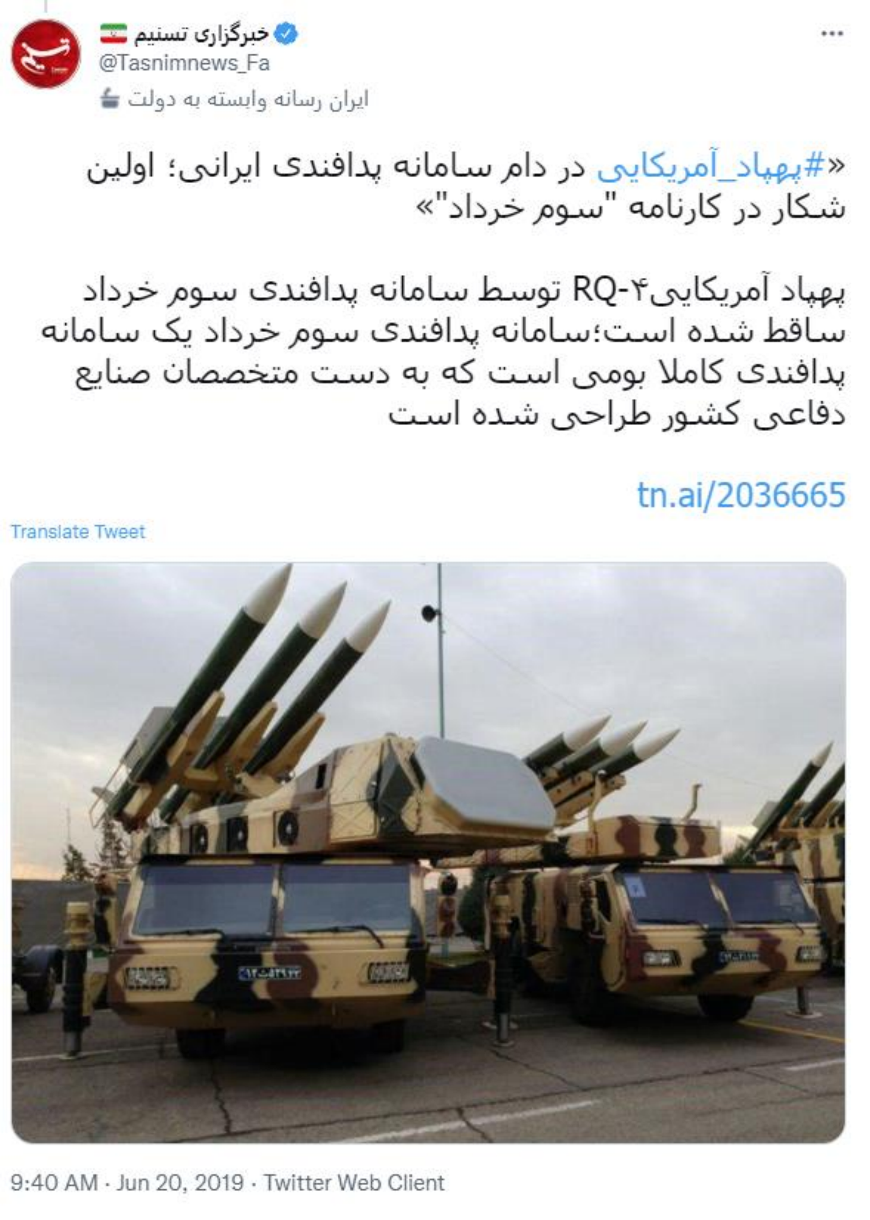
https://twitter.com/RedFox0x20/status/1485237440080191490?s=20&t=tUun6pcpAs1Pc6CuW_NdJg
https://twitter.com/RedFox0x20/status/1485237894449086466?s=20&t=tUun6pcpAs1Pc6CuW_NdJg


Russian cluster strikes
UA Air Defense
RU high caliber arty

Attacks that Deny Information



Attacker destroys or otherwise disrupts the Receiver



خبرگزاری تسنیم
@Tasnimnews_Fa
ایران رسانه وابسته به دولت

«#پهپاد_آمریکایی در دام سامانه پدافندی ایرانی؛ اولین
شکار در کارنامه "سوم خرداد"»

پهپاد آمریکاییRQ-۴ توسط سامانه پدافندی سوم خرداد
ساقط شده است؛سامانه پدافندی سوم خرداد یک سامانه
پدافندی کاملا بومی است که به دست متخصصان صنایع
دفاعی کشور طراحی شده است

tn.ai/2036665

Translate Tweet

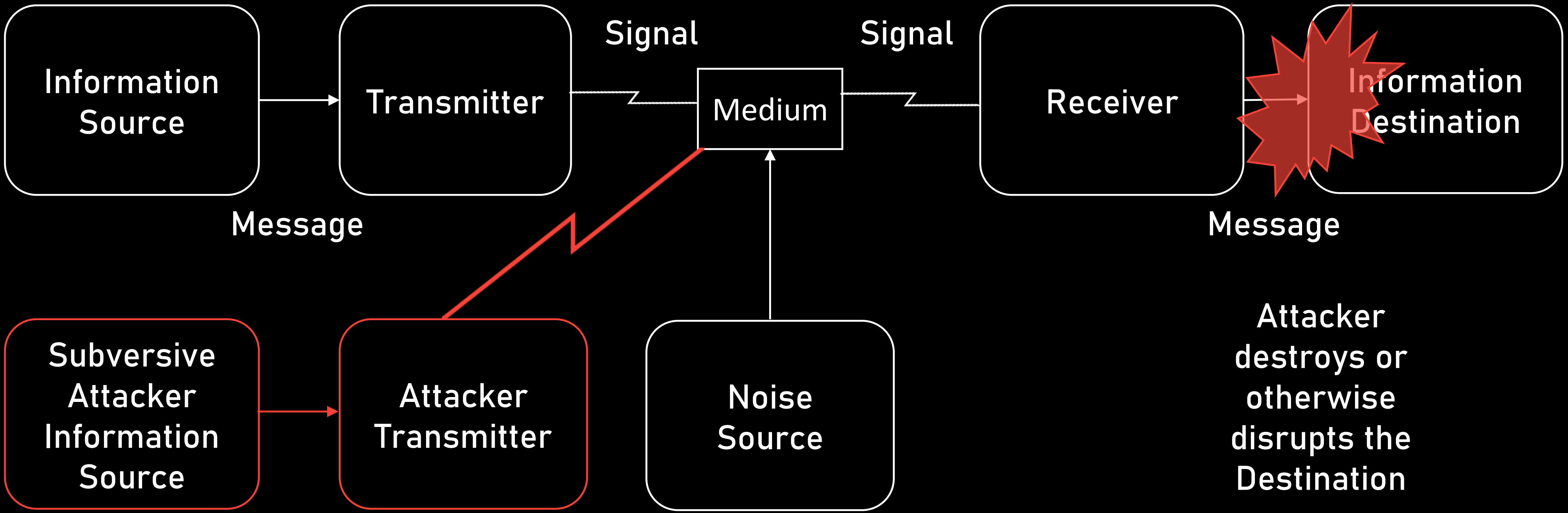
9:40 AM · Jun 20, 2019 · Twitter Web Client

An additional breach, according to one person briefed on the operations, targeted other computer systems that control Iranian missile launches.

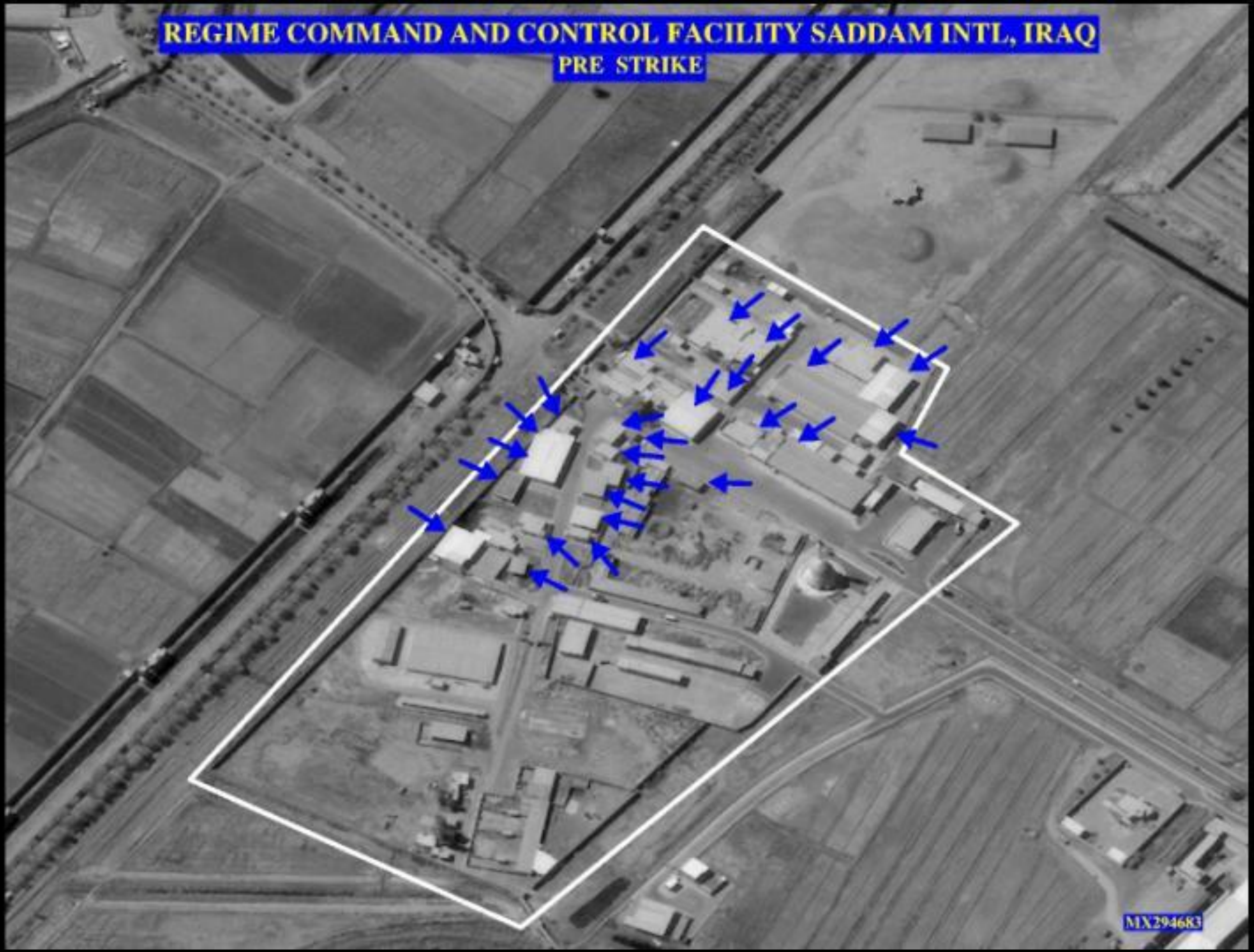
https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html

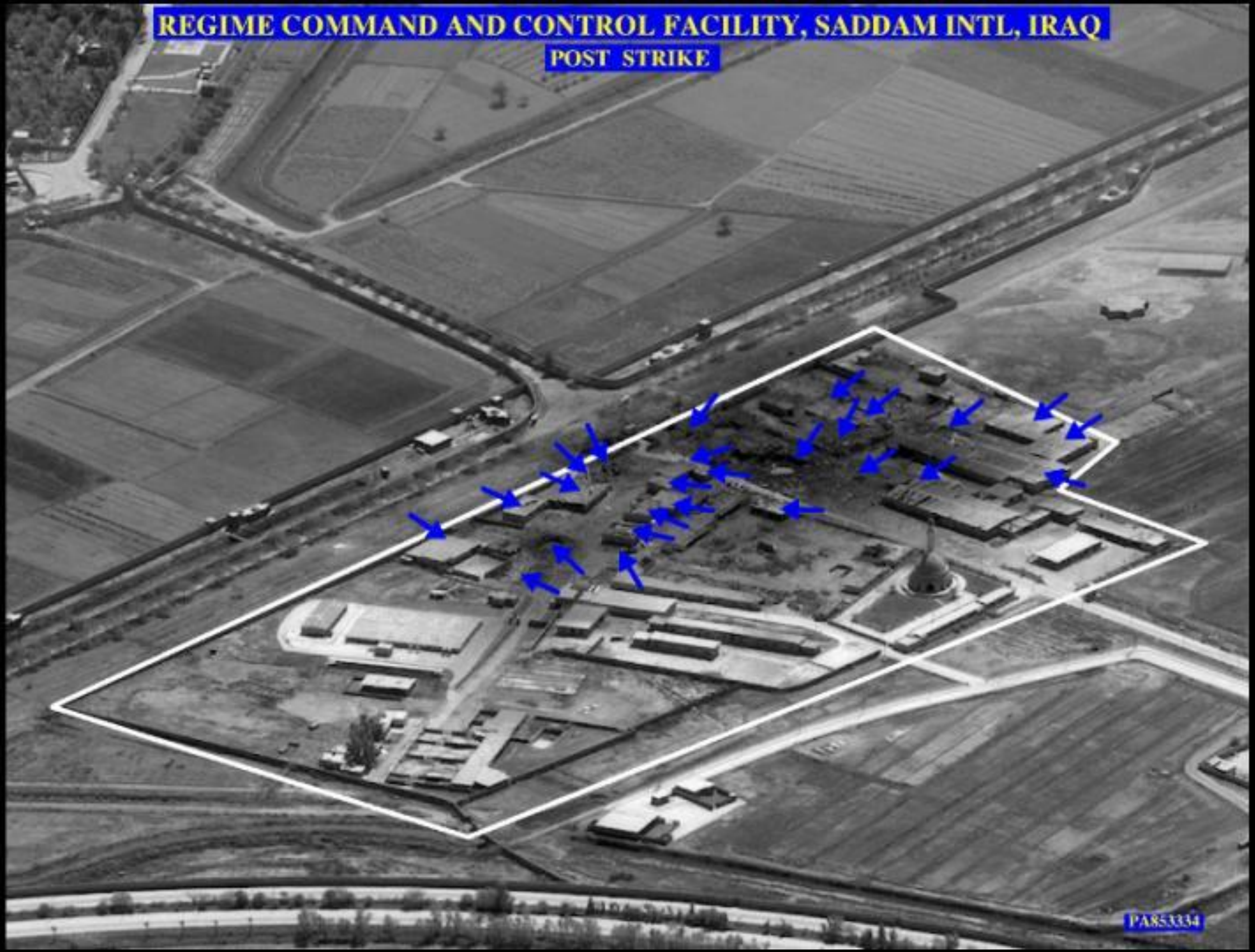
5302 K8

Attacks that Deny Information



Attacker destroys or otherwise disrupts the Destination





https://nsarchive2.gwu.edu/NSAEBB/NSAEBB88/

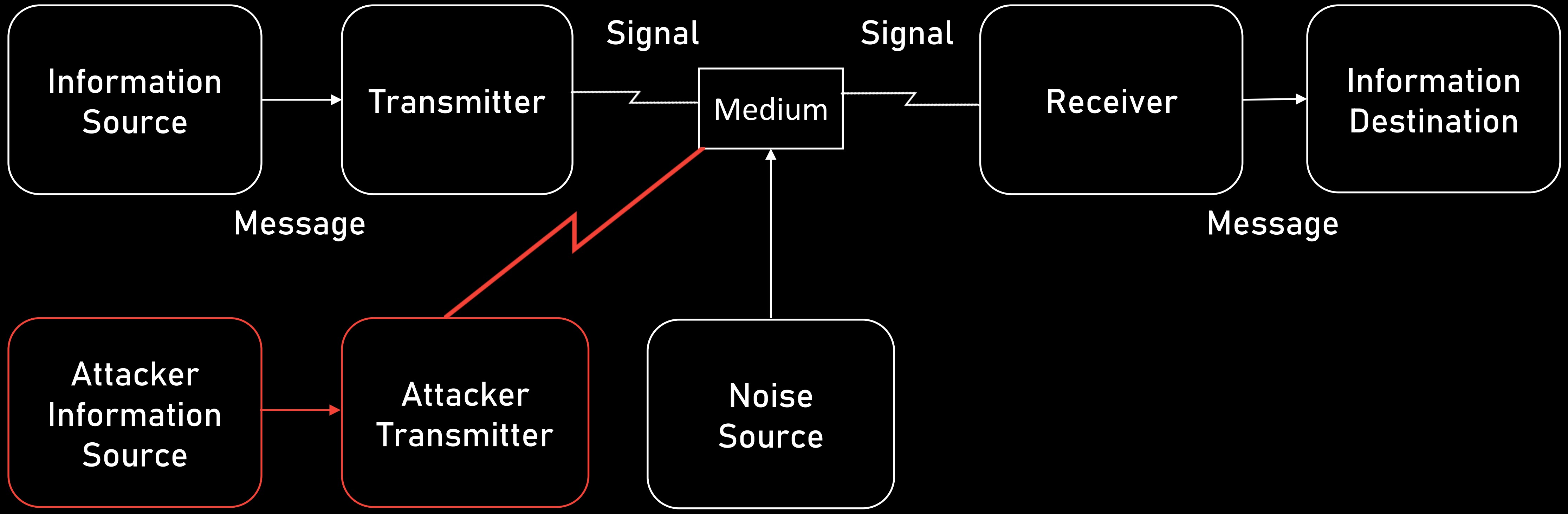
https://twitter.com/LostWeapons/status/1502414061010522112?s=20&t=vBYqwy-xwBH4IcSXtVx_dw

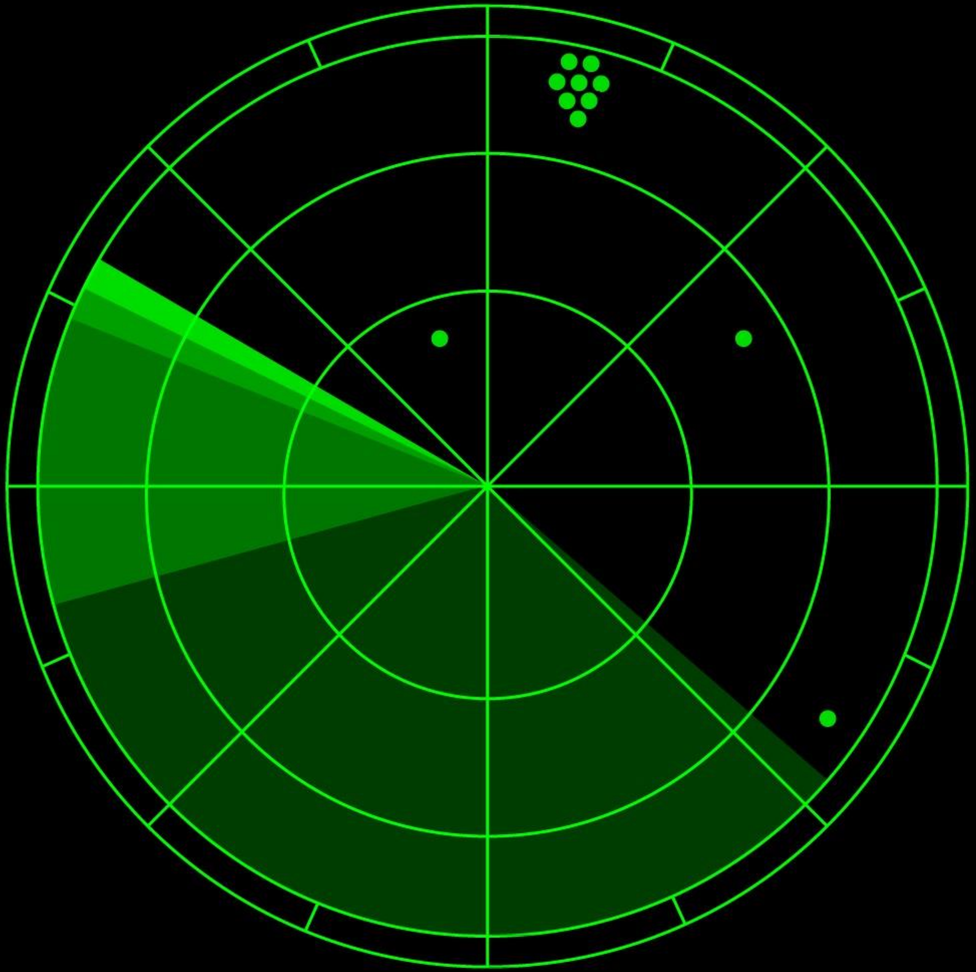
MAJ GEN

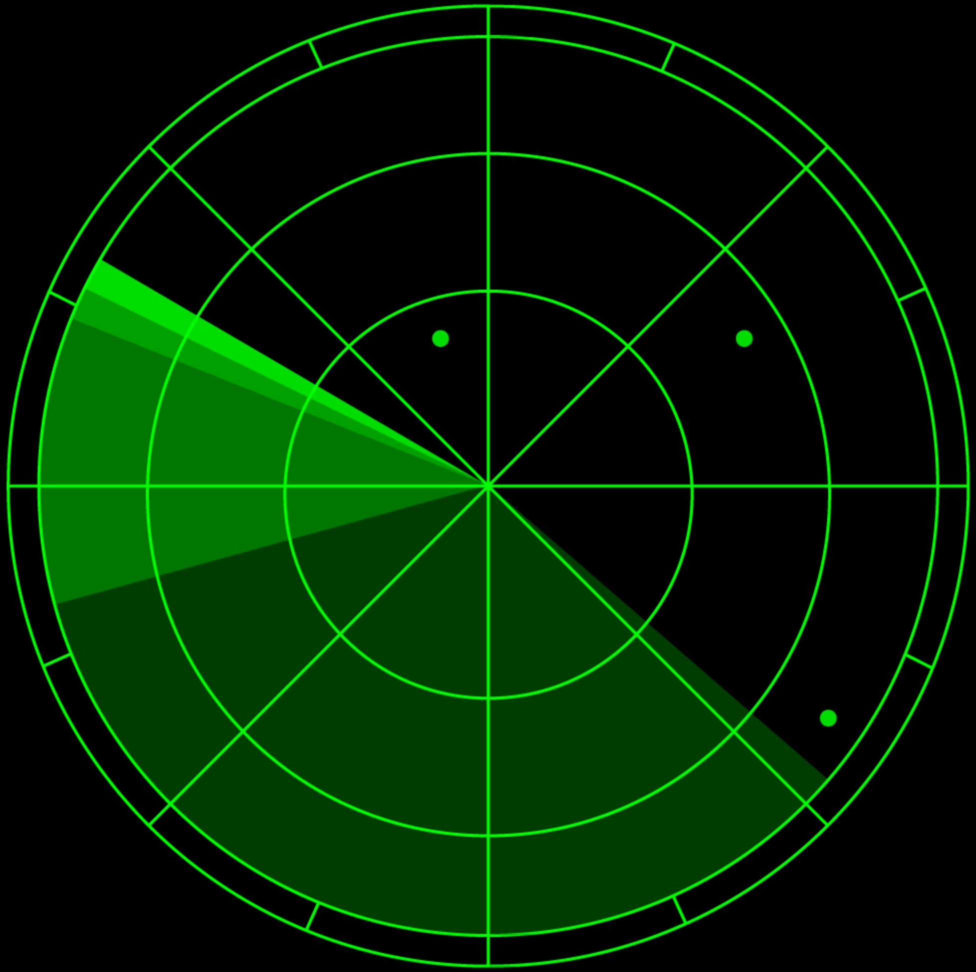
COL

LT COL

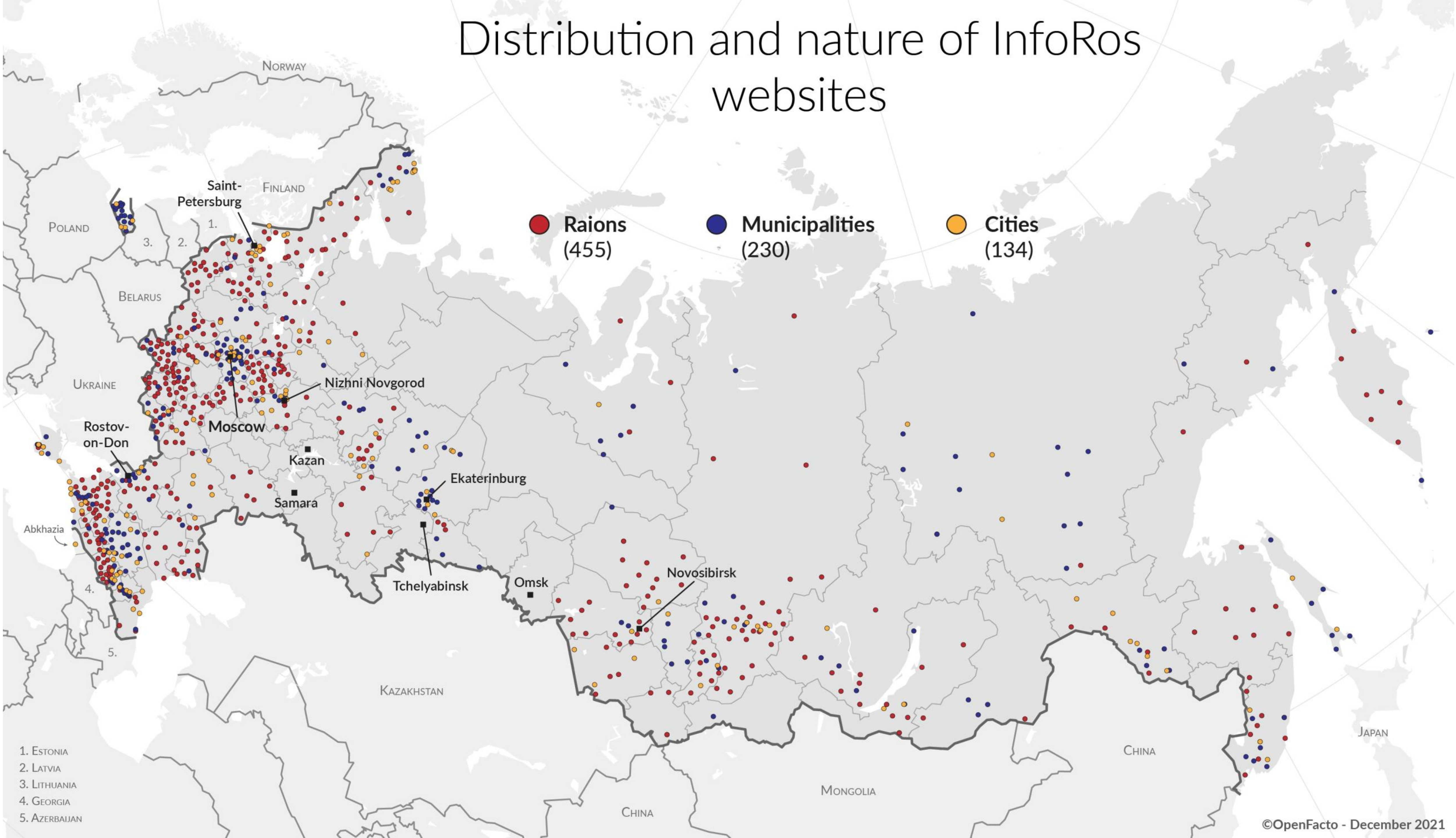
Attacks that Corrupt Information Sources



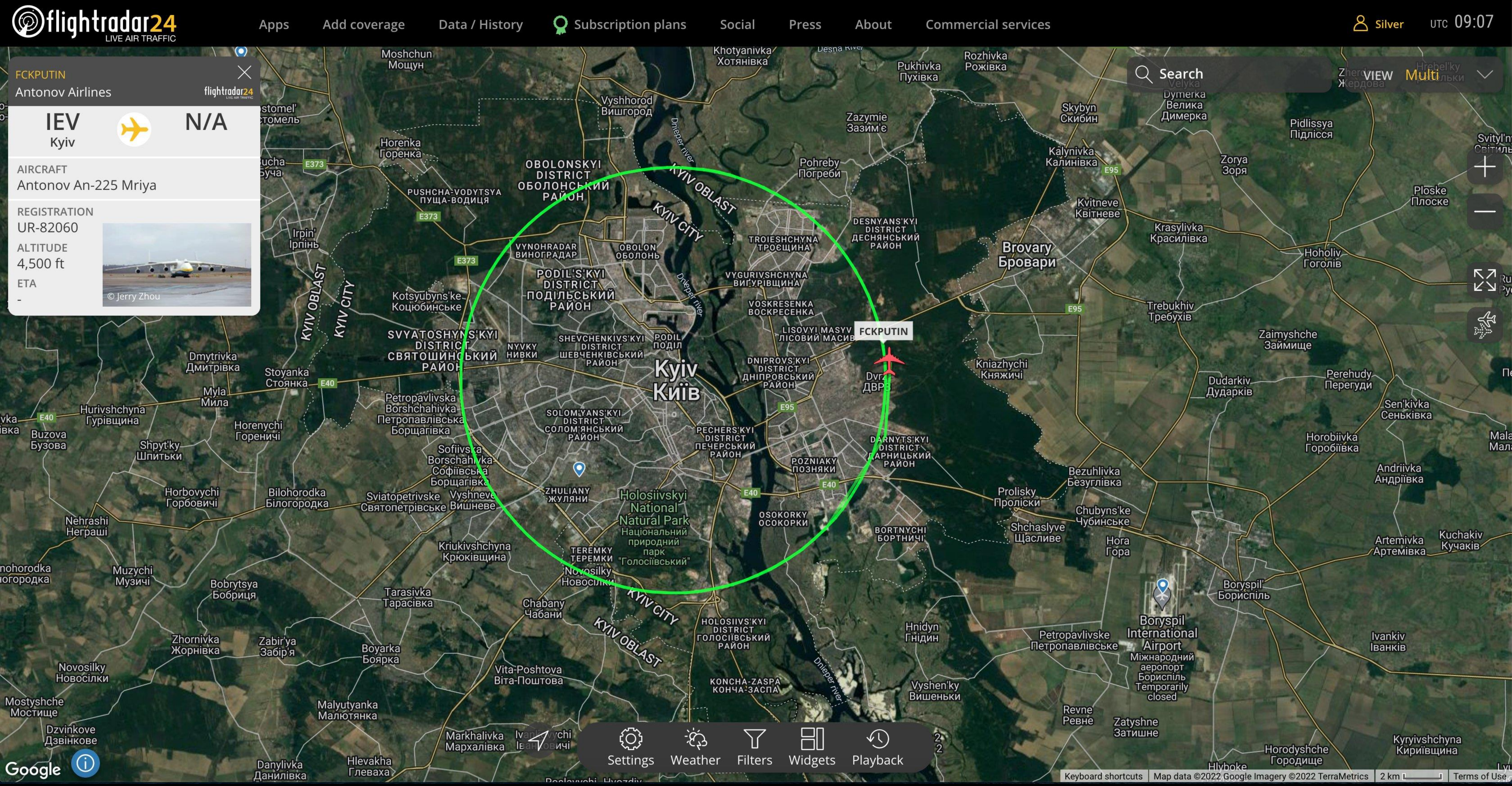




Distribution and nature of InfoRos websites



©OpenFacto - December 2021



FCKPUTIN

Antonov Airlines

IEV Kyiv → N/A

AIRCRAFT
Antonov An-225 Mriya

REGISTRATION
UR-82060

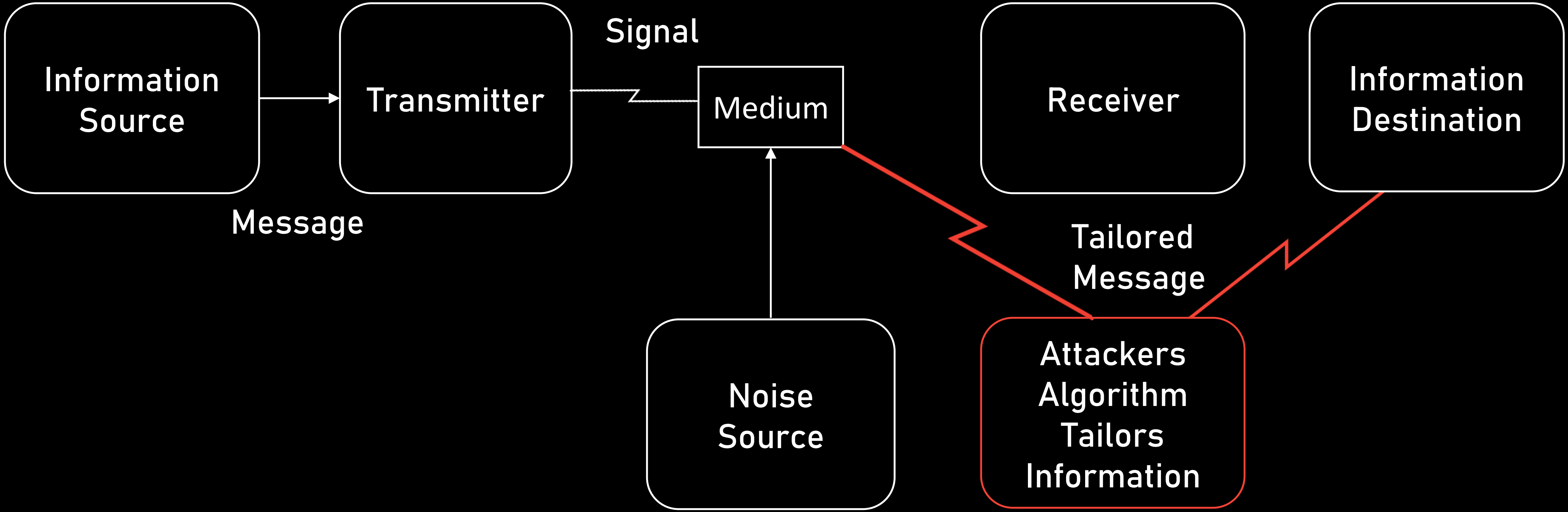
ALTITUDE
4,500 ft

ETA
-

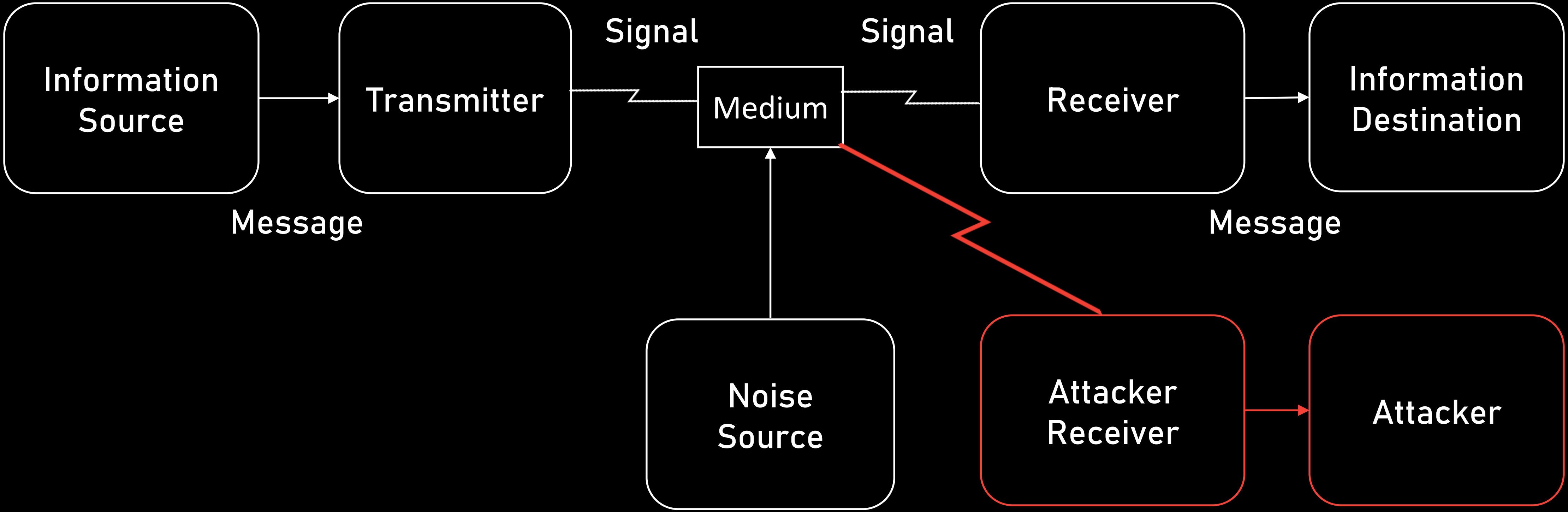
© Jerry Zhou

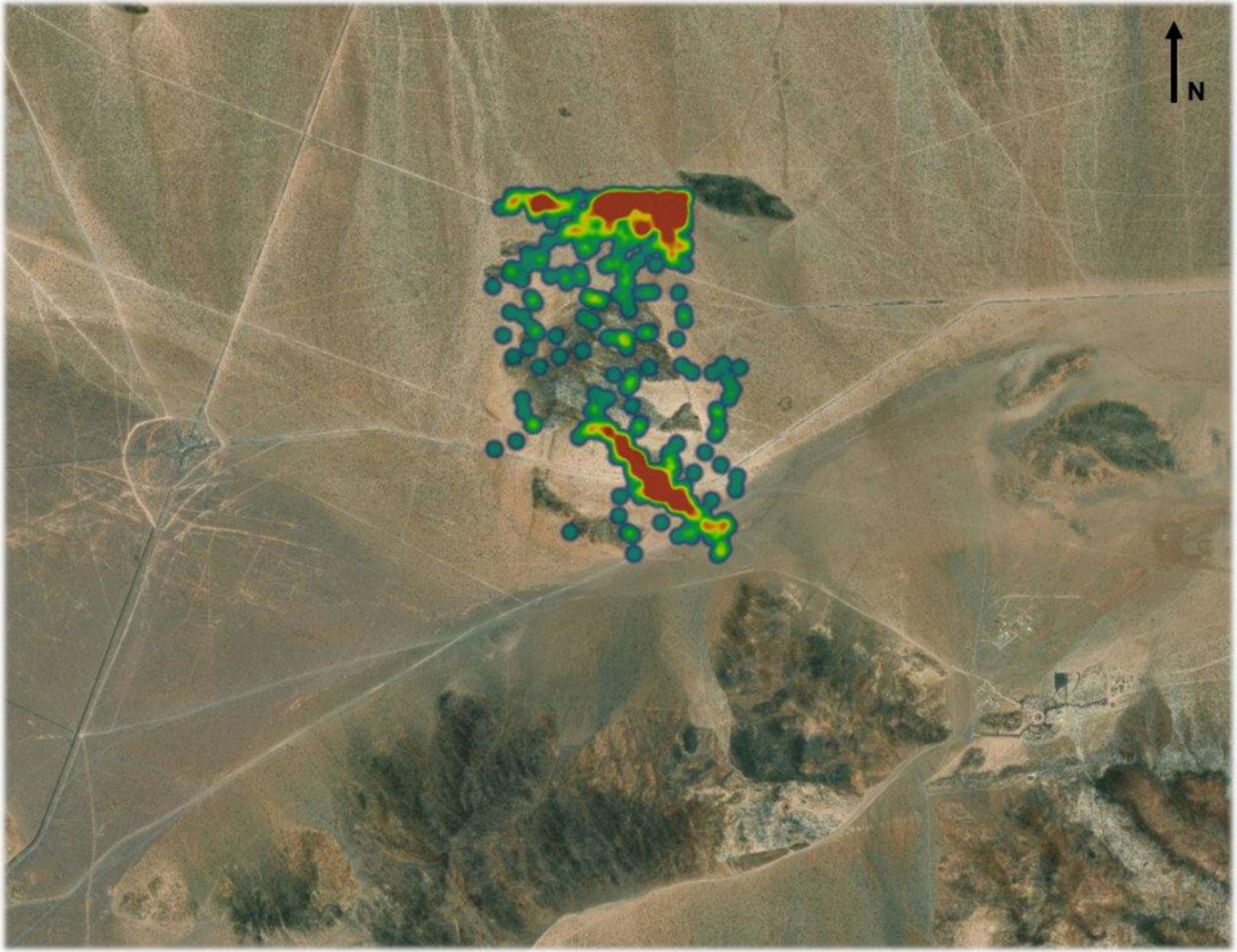
UTC 09:07

Attacks that Corrupt Information Sources

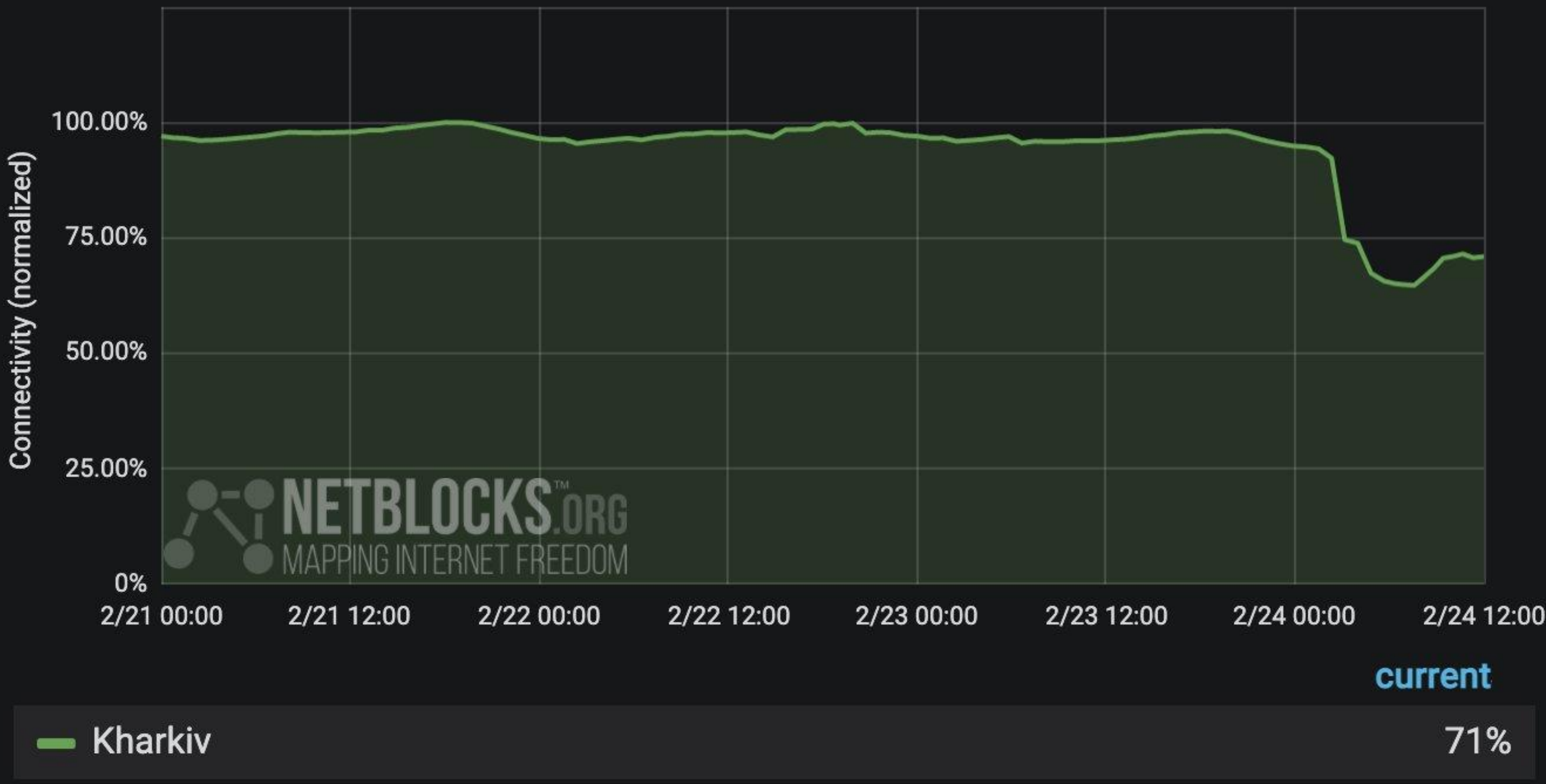


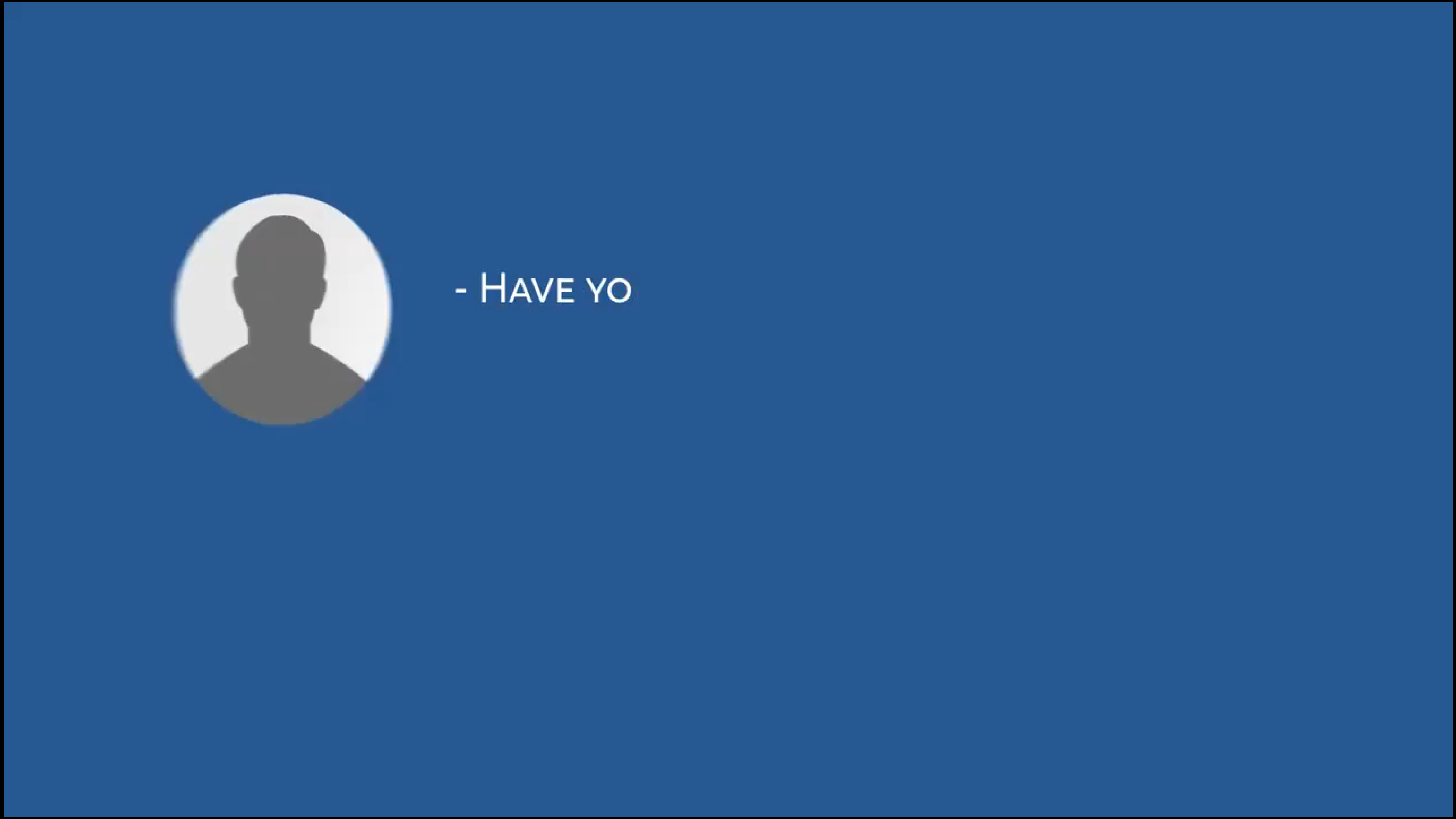
Attacks that Exploit Information



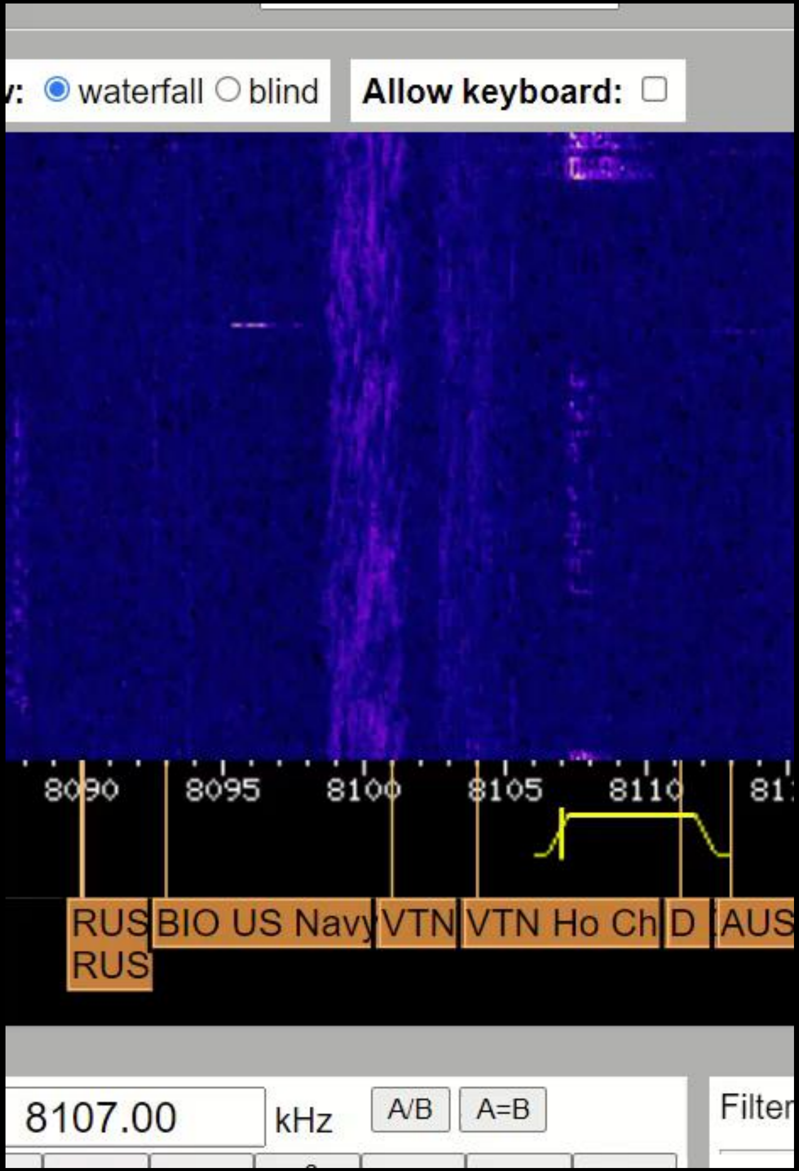

N

Network Connectivity - Selected Regions, Ukraine: 2022-02-21 to 2022-02-24 UTC





https://youtu.be/LYumd3pt9F8?start=166&end=227



:● waterfall ○ blind

Allow keyboard: □

8107.00 kHz

Yes, I can ??? you, ???

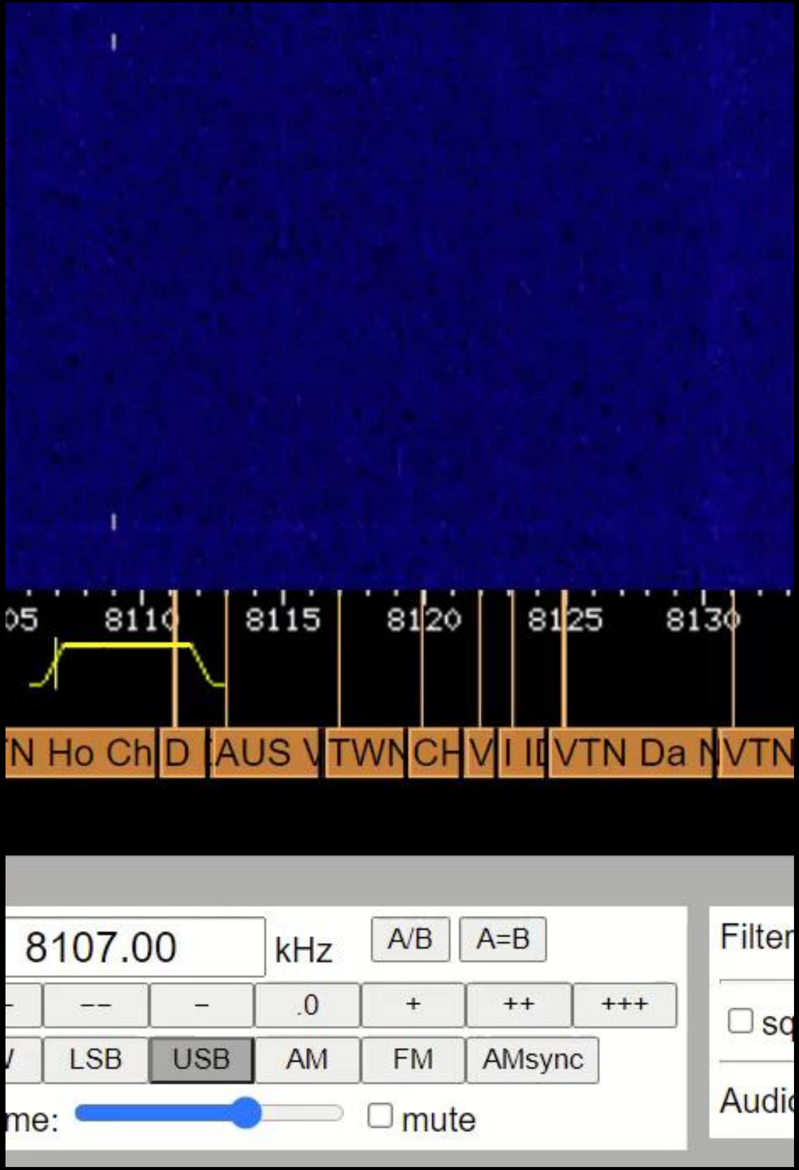
Ryazan I’m ??? (portrait?), over

??? (Portrait?), I’m Ryazan, over

Ryazan, [we are] working on the 16th ???

Continue to work on this route, everyone stay alert [via radio], I’m Ryazan

Roger that, over



8107.00 kHz

USB

I'm Ryazan, over

I'm Uragan, over

Uragan, I'm Ryazan, over

How… can we… transmit data, or receive it? over

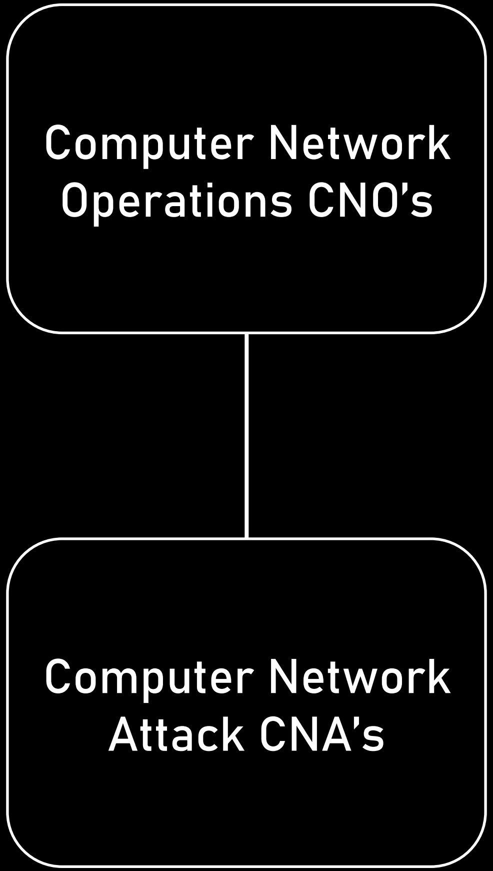
(bleeping)

Ryazan, I'm Geyzer, ???

Geyzer, Geyzer, I'm Ryazan, over

I'm Geyzer, will clarify how Uragan can pass data and receive it, over

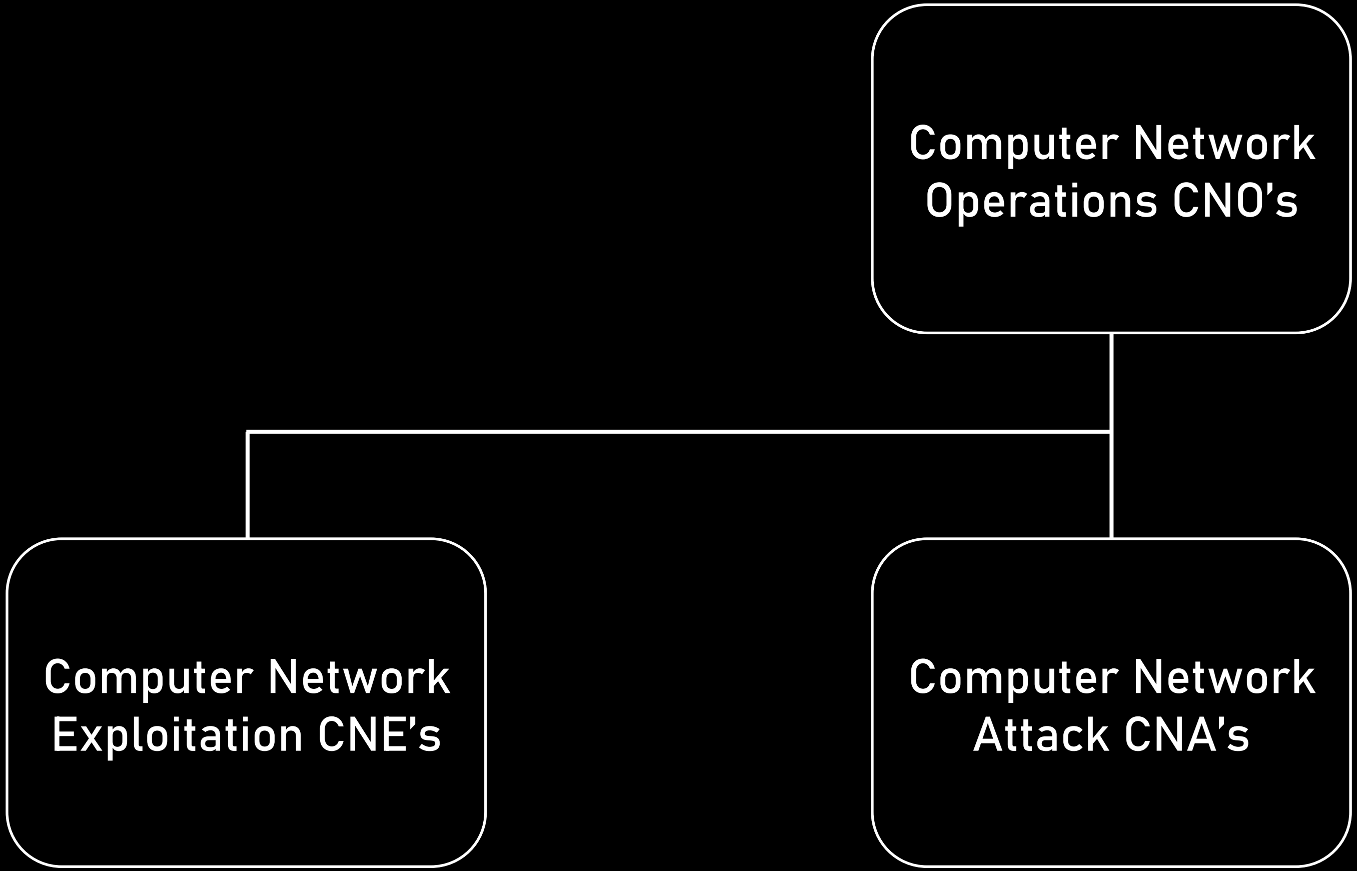
Computer Network Operations



Computer Network Operations CNO's

Computer Network Attack CNA's

Computer Network Operations

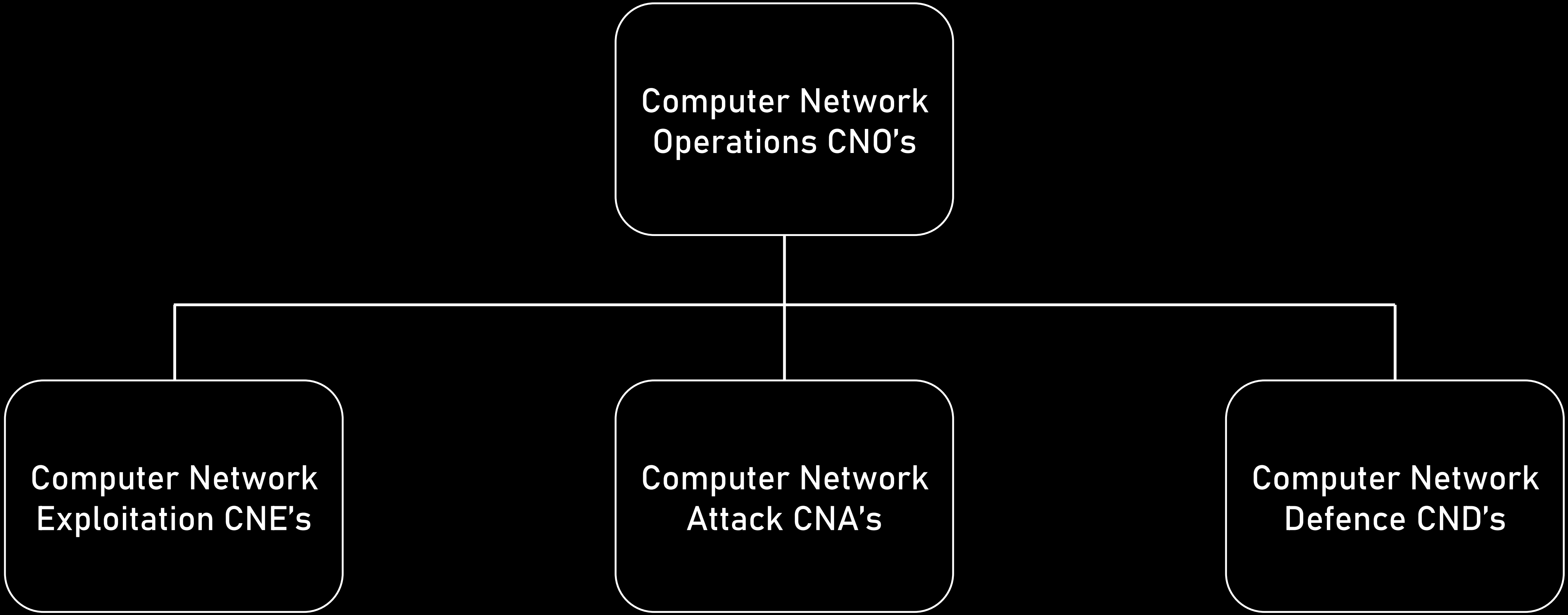


Computer Network Operations CNO's

Computer Network Exploitation CNE's

Computer Network Attack CNA's

Computer Network Operations



Computer Network Operations CNO's

Computer Network Exploitation CNE's

Computer Network Attack CNA's

Computer Network Defence CND's

Battlefield Shaping

Nov 2021 USCYCOM deployed Cyber Mission Teams to Ukraine

Jan 2022 NSA issues Advisory on protecting VSAT equipment

Dragos detects INDUSTROYER and BLACKENERGY in Jan & Feb

MSFT MISTIC detects WhisperGate Wiper

ESET detects HermeticWiper

Microsoft detects FoxBlade at H Hour and patchs within 3 hours

Fortinet DDoS “Virtual Machine” to protect Ukrainian Police

https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471

So Where Is The Cyberz Pew Pew?

- Cyber isn’t magic
- Cyber takes time and investment to prepare and preposition, Russia lacked all of this
- Believe it or not, Cyber has limitations
- People have been thinking about these problems for millennia
- Cyber is just one of a range of options available to militaries
- Sometimes things that go bang or boom are just more effective
- The insane defensive efforts aren’t sexy thus are unreported

Q&A

Acknowledgements

Thanks to Tinfoil, Jack and aminal for war gaming ideas, finding documents and things I forgot about, and for the craic!

Microbiote made me some rad graphics! So thanks mate😁

David, my Signals Officer, for the Radio Intercepts

Victor, my Cryptographic Linguist, for translations

Sinan for Linguistic Support

The Irish Cyber Security And Privacy Community Discord

@LegendaryPatMan

paddy@cyberwarfa.re