Cyber island

November 2020 - January 2021

US Army Vs Armed Forces of the Russian Federation

Carte : Napf

Document version : 1.0
Last Edition : 07/11/2020

English version

Summary

Features

- ➔ 5 missions defined in advance every 2 weeks.
- ➔ 2 Hours of mission + 15 minutes of IN GAME Briefing (unless exemption mentioned by DOJ).
- ➔ No reappearance.
- ➔ OB Imposed by DOJ.
- ➔ Various objectives.
- ➔ Campaigns at 50 points, 10 points per mission.
- ➔ The camp with the most points after the 5 missions wins the campaign!

Règles de jeu

- **OFCRA rules apply for the campaign.**
- Any request for a change of mission must be made 5 days before the date on which the mission will be played.

Modset « Cyber island »

1. *@ace*
2. *@ace_compat_rhs*
3. *@acex*
4. *@CBA_A3*
5. *@CUP_Terrains_Core*
6. *@Napf_island_a3*
7. *@niarms_ak*
8. *@niarms_compat_rhs*
9. *@niarms_core*
10. *@ofcra_v3*
11. *@RHSAFRF*
12. *@RHSGREF*
13. *@RHSUSAF*
14. *@tfar*

Calendrier

Mission	Date	Start Time
M01 - « Wassenaar »	November 2020	**21:00 (Paris)**
M02 - « Vernam »	December 2020	
M03 - « Hellman »	January 2021	
M04 - « ROT47 »	January 2021	
M05 - « Euler Indicator »	February 2021	

NB : The dates given here are subject to change! In this case, the actors will be notified.

Contacts

Campaign Managers

The managers are listed in the following table :

Name	Role	Preferred method of contact	Comment
Flip4Flap	Président OFCRA CDC	Forum OFCRA Discord	For any question relating to attendance and organizational arrangements.
Manchot	Server Administrator in charge of diplomatic relations Member of the board		
Mrwhite350	MJ Member OFCRA CDG	Forum OFCRA	For any question related to missions (additional info, ACE tuning, difficulty ...), loadouts.

Canaux de communication

It is possible to contact the people listed above by using the means below and in order of priority:

1. OFCRA Forum > https://ofcrav2.org/forum/index.php?action=forum
    1. If it is confidential information, go through a private message.
    2. If it is public information, go through the campaign topic provided for this purpose.
2. OFCRA Discord > https://discord.gg/bWtGS7N
    1. Either by direct message to the campaign managers
    2. Either in the "general" channel
3. By Steam message to each protagonist

Scoreboard

Mission	Points per mission
M01	10
M02	10
M03	10
M04	10
M05	10
Total	50

Légende

- **Violet** : common objective of the 2 camps
- **Red**: REDFOR lens
- **Blue**: BLUEFOR lens

Ruban de campagne

The campaign ribbon is made by Manchot.

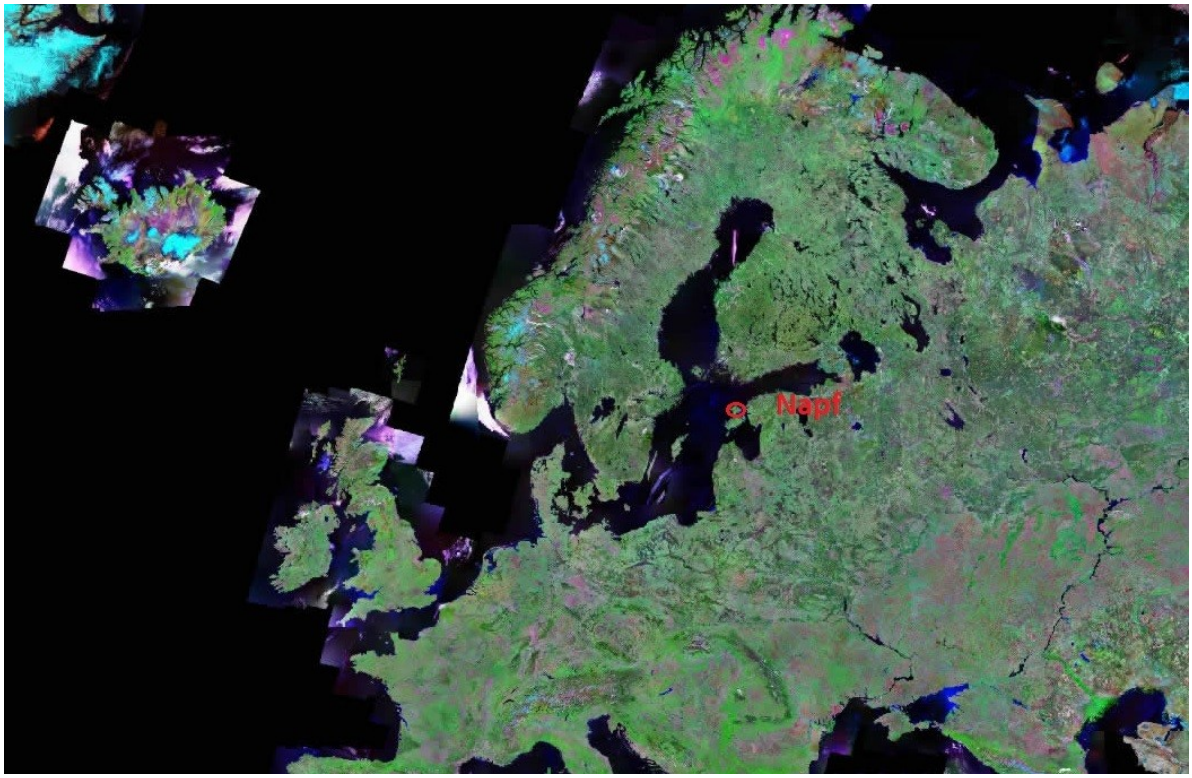
Sitac

Following the massive computer attack that targeted Estonia in 2007. The various major powers have understood the importance of cyberspace in international issues and armed conflicts. In fact, all states have now invested in offensive cyber warfare (LIO) capabilities. The USA and the Russian Federation are coming out, as usual, their pinnacle of the game thanks to early anticipation and longstanding expertise.

Computer warfare (also known as cyberwarfare) is a very interesting field of confrontation: the concealment of traces is easy, the identification of actors is opaque, the costs of operations are reduced, and it is possible to attack any adversary directly on its territory without carrying out military maneuvers.

In 2012, in response to the disclosure of sensitive information by pirate groups presumably affiliated to the FSB (mainly Fancy Bear and Cozy Bear) the US strengthened its signal interception capabilities. Their main base is located on the island of Napf.

The island has the particularity of being very well placed to intercept the low frequency signals that are emitted by the Russians from the Kaliningrad area. Estonia also has a long tradition of signal interception and electronic warfare: it was from this country that the Soviets intercepted most of the military communications across the Iron Curtain.



Since Estonia's integration into NATO, the military installations in Napf have been made available to the Americans, who can conduct operations there from the Estonian side.

The Kremlin sees Napf as its pre-square where it can also station troops. To do this, the Russians exploit a legal loophole in the treaty that made Estonia independent at the time of the fall of the Soviet empire.

This stationing of Russian and American forces on the same territory is not quick to ease tensions in the Baltic Sea. Paradoxically, both sides use this proximity to their advantage: it is much simpler to intercept electronic signals and conduct cyber operations: the submarine cable linking Napf to the global internet network is unique. All connections (outside the military networks), coming from the Russian or Estonian side, transit through the same channel, making it very difficult to attribute an attack.

The island has become a paradise for any self-respecting hacker and each side has set up its own specialised regiments there: elements of the 780th Military Intelligence Brigade for the USA and sections of the Russian Spetssviaz. In addition to the military forces, each camp tolerates pirates identified as "independent" and private military companies specialising in the IHL are also installed, each acting opaque on behalf of one camp.

However, things changed in 2013. An attack targeting vital systems in the US was successfully countered, traces were recovered and forensic analysis showed that the modus operandi was very (too) similar to the brand of a Russian hacker group.

The investigations continued until DRM intercepted a telephone message: the hacker in charge of the operation was selling his girlfriend on a trip to Paris on the results of his hacking and the very high remuneration he had been offered by the FSB.

The French, having a long history of collaboration within NATO, notified the American administration of his discovery while providing the audio recording, which was very explicit.

The US, too happy to exploit this information, called Russia to account. Russia, highly discredited on the diplomatic scene, did not respond.

Faced with this silence, the US decided to exploit this temporary weakness in order to silence cyber operations on the island of Napf by launching a military operation, officially to track down and recover the group of hackers responsible for the attack.

The Russians, unimpressed, put all their military units stationed on the island on alert.

Camps

USA

Russian Federation

Loadouts

The loadouts are freely available at this address:

https://github.com/ofcrav2/omtk/tree/master/omtk-loadouts/infantry

In the event of a significant change, information will be provided by the DOJ on the OFCRA forum.

End of Document