Cyber island

Novembre 2020 – Janvier 2021

US Army Vs Armed Forces of the Russian Federation

Carte : Napf

Version du Document : 1.0
Date de dernière Édition : 07/11/2020

Version française | Diffusable

Sommaire

Features

- ➔ 5 missions définie à l'avance toutes les 2 semaines.
- ➔ 2 Heures de mission + 15 minutes de Briefing IN GAME (sauf exemption mentionné par le MJ).
- ➔ Pas de réapparition.
- ➔ OB Imposé par le MJ.
- ➔ Objectifs variés.
- ➔ Campagnes à 50 points, 10 points par mission.
- ➔ Le camp possédant le plus de point à la suite des 5 missions remporte la campagne !

Règles de jeu

- **Les règles de l'OFCRA s'appliquent pour la campagne.**
- Toute demande de modification de mission doit se faire 5 jours avant la date ou la mission sera jouée.

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 »	Novembre 2020	**21:00 (Paris)**
M02 - « Vernam »	Décembre 2020	
M03 - « Hellman »	Janvier 2021	
M04 - « ROT47 »	Janvier 2021	
M05 - « Euler Indicator »	Février 2021	

NB : Les dates données ici sont susceptibles de changer ! Dans ce cas, les acteurs seront prévenus.

Contacts

Gestionnaires de la campagne

Les gestionnaires sont listés dans le tableau suivant :

Nom	Rôle	Mode de contact préféré	Commentaire
Flip4Flap	Président OFCRA CDC	Forum OFCRA Discord	Pour toute question relative aux présences et modalités d'organisation.
Manchot	Administrateur serveur Chargé relation diplomatiques Membre du bureau		
Mrwhite350	MJ Membre OFCRA CDG	Forum OFCRA	Pour toute question relative aux missions (infos supplémentaire, réglage ACE, difficulté …), loadouts.

Canaux de communication

Il est possible de contacter les personnes listées précédemment en utilisant les moyens ci-dessous et par ordre de priorité :

1. Forum de l'OFCRA > https://ofcrav2.org/forum/index.php?action=forum
    1. Si c'est une information confidentielle, passer par un message privé.
    2. Si c'est une information publique, passer par le topic de campagne prévue à cet effet.
2. Discord de l'OFCRA > https://discord.gg/bWtGS7N
    1. Soit par message direct aux gestionnaires de la campagne
    2. Soit dans le canal « général »
3. Par message Steam à chaque protagoniste

Tableau des scores

Mission	Points par mission
M01	10
M02	10
M03	10
M04	10
M05	10
Total campagne	50

Légende

- **Violet :** objectif commun aux 2 camps
- **Rouge :** objectif REDFOR
- **Bleu :** objectif BLUEFOR

Ruban de campagne

Le ruban de campagne est réalisé par Manchot.

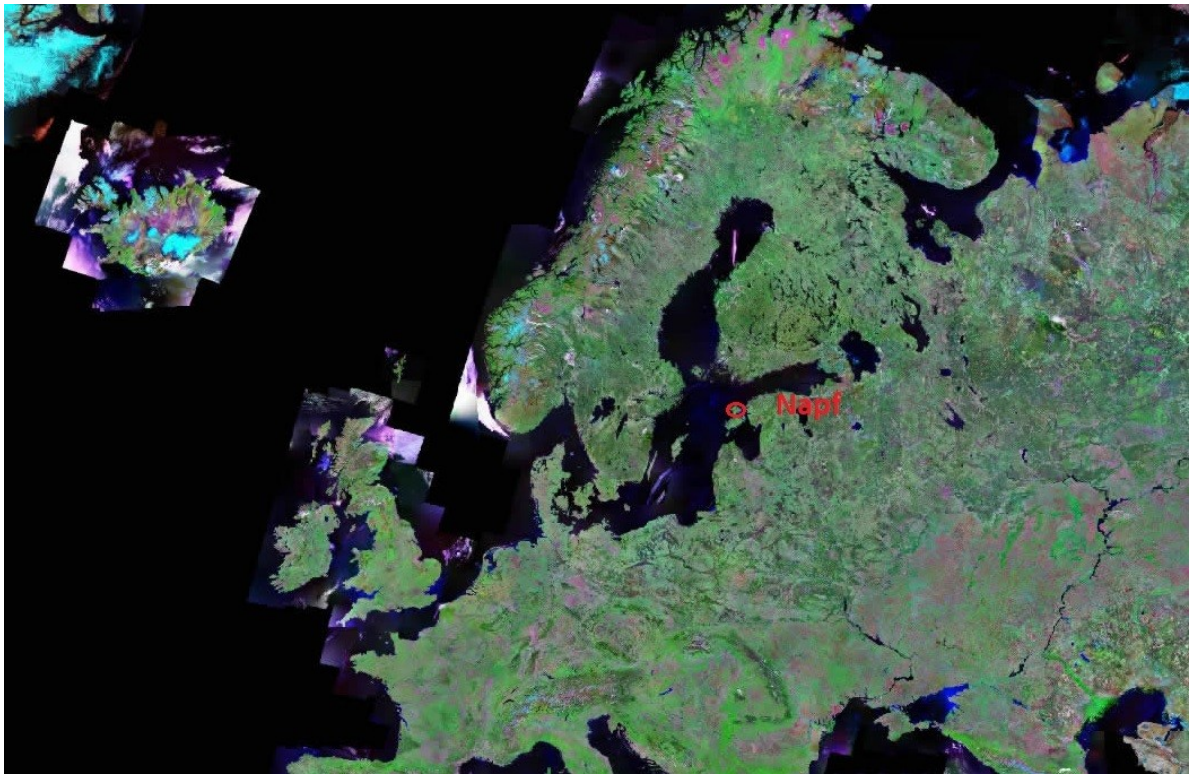
Sitac

Suite à l'attaque informatique massive ayant visé l'Estonie en 2007. Les différentes grandes puissances ont compris l'importance qu'a pris le cyberespace dans les enjeux internationaux et les conflits armés. De fait tous les états ont maintenant investi dans des capacités de lutte informatique offensive (LIO). Les USA et la Fédération de Russie sortant, comme d'habitude leur épingle du jeu grâce à une anticipation précoce et une expertise de longue date.

La lutte informatique (aussi nommé Cyberguerre) est un champ d'affrontement très intéressant : la dissimulation des traces est aisée, l'identification des acteurs opaques, les coûts des opérations sont réduits et il est possible d'attaquer n'importe quel adversaire directement sur son territoire sans effectuer de manœuvres militaires.

En 2012, en réponse à la divulgation d'information sensibles par des groupes de pirates vraisemblablement affilié au FSB (*principalement Fancy Bear et Cozy Bear*) les USA ont renforcés leurs moyens d'interception de signaux. Leur base principale est située sur l'île de Napf.

L'île possède la particularité d'être très bien placé pour intercepter les signaux de basse fréquences qui sont émis par les Russes depuis l'enceinte de Kaliningrad. L'Estonie à également une longue tradition dans l'interception de signaux et la guerre électronique : c'est depuis ce pays que les Soviétiques interceptaient la majorité des communications militaire de l'autre côté du rideau de fer.



Depuis l'intégration de l'Estonie au sein de l'OTAN, les installations militaires de Napf sont mises à disposition des Américains qui peuvent y mener des opérations depuis la partie Estonienne .

Fort d'une ancienne tradition russe, le Kremlin voit Napf comme son pré-carré ou il peut également stationner des troupes. Pour ce faire, les Russes exploitent un flou juridique dans le traité qui rendait l'Estonie indépendante lors de la chute de l'empire soviétique.

Ce stationnement de forces russes et Américaine sur le même territoire n'est pas prompt à apaiser les tensions dans la mer Baltique. Paradoxalement, les deux camps utilisent cette proximité pour en tirer un avantage : il est bien plus simple d'intercepter des signaux électroniques et de mener des opérations cyber : le câble sous marin reliant Napf au réseau internet mondial est unique. Toutes les connexions (en dehors des réseaux militaires), provenant de la partie russe ou Estonienne transitent vers le même canal, rendant très difficile l'attribution d'attaque.

L'île est devenue le paradis pour tout hacker qui se respecte et chaque camp y a installé ses régiments spécialisés : des éléments de la *780th Military Intelligence Brigade* pour les USA et des sections de la *Spetssviaz* Russe. Outre les forces militaires, chaque camp tolèrent des pirates identifiés comme « indépendant » et des sociétés militaires privées spécialisée dans la LIO sont également installées, chacune agissement opaquement pour le compte d'un camp.

Toutefois, les choses changèrent en 2013. Une attaque ayant visé des systèmes vitaux aux USA a réussie à être contrée, les traces ont été récupérées et les analyses forensic ont démontrés que le mode opératoire était très (trop) ressemblant à la marque d'un groupe de hacker russe.

Les investigations continuèrent jusqu'à que la DRM intercepte un message téléphonique : le hacker en charge de l'opération se ventait auprès de sa petite amie en voyage à Paris des résultats de son piratage et de la rémunération très élevé que lui avait offert le FSB.

Les Français, possédant une longue histoire dans la collaboration au sein de l'OTAN avisa l'administration américaine de sa découverte tout en fournissant l'enregistrement audio, très explicite.

Les USA, trop content de pouvoir exploiter cette information, ont sommé la Russie de rendre des comptes. La Russie, fortement décrédibilisée sur la scène diplomatique n'a pas répondu.

Face à ce silence, les USA ont décidé d'exploiter cette faiblesse temporaire afin de réduire au silence les opérations cyber sur l'île de Napf en lançant une opération militaire, officiellement pour traquer et récupérer le groupe de pirates responsable de l'attaque.

Les Russes, nullement impressionné, mettent en alerte toutes leurs unités militaires stationnées sur l'île.

Camps

USA

Russian Federation

Loadouts

Les loadouts sont librement consultables à cette adresse :

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

En cas de changement notable, une information sera donnée par le MJ sur le forum de l'OFCRA.

Fin de Document