RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

KIT CYBER en JEUX

Formez à la cybersécurité par le jeu

par l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI) et le 110 bis, lab d'innovation de l'Éducation nationale.

Version bêta - juin 2021

110 bis Lab de l'éducation nationale

La démarche

Dans un contexte conjuguant augmentation des risques cyber pour les citoyens, les institutions publiques et les acteurs économiques et déficit de spécialistes en la matière, la formation aux enjeux et métiers de la sécurité numérique est clé.

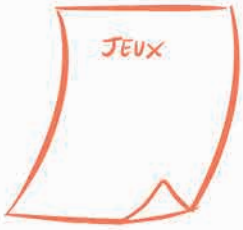
En 2019, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et le ministère de l'Education nationale, de la Jeunesse et des Sports (MENJS) ont uni leurs forces dans le cadre de l'initialisation d'une feuille de route conjointe intitulée « Cybersécurité : former et susciter des vocations » .
Parmi les axes de travail identifiés : l'élaboration de ressources pédagogiques et d'outils d'apprentissage innovants, notamment au travers du jeu.

C'est tout l'objet de ce kit, co-élaboré par le pôle innovation de l'ANSSI et le 110 bis, lab d'innovation de l'Education nationale : faciliter la création de jeux sérieux pour former les jeunes à la cybersécurité.

Ce kit a été imaginé comme un support pratique à la création et la mise en commun de jeux sérieux destinés, en premier lieu, aux élèves du secondaire. Vous y trouverez toutes les étapes pas-à-pas de conception et d'organisation d'une séquence de création de jeux sérieux, sur une journée ou sur plusieurs semaines.

Néanmoins, parce que la cybersécurité nous concerne tous, ce kit a été pensé pour être adapté au public le plus large possible. Il peut donc également être utilisé pour la création de jeux destinés aux professionnels, étudiants, par exemple dans le cadre de la formation supérieure ou continue ou encore à des fins de sensibilisation au risque numérique.

Contenu du kit

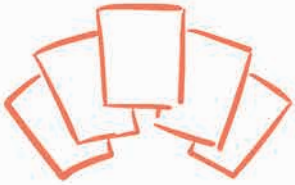


2 fiches « jeux » pour comprendre les ressorts des jeux sérieux

Présentant différents types de jeux sérieux et leur utilité en matière d'apprentissage.

4 fiches « organisation » pour concevoir et piloter une séquence de création de jeux sérieux

Détaillant concrètement les étapes de la conception, de l'organisation et de l'animation d'une séquence de création de jeux sérieux impliquant des participants.



10 cartes « objectifs pédagogiques »

Présentant les objectifs d'apprentissage, au choix, des jeux destinés aux élèves.

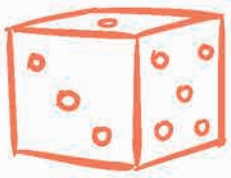
14 fiches « cybersécurité »

Permettant à des participants adultes à une séquence de création de jeux sérieux ou à ses organisateurs de se familiariser aux enjeux de cybersécurité.

Dans le cas où le kit est utilisé comme support à une séquence pédagogique, ces fiches peuvent constituer une base de ressources sur lesquelles les enseignants ou les formateurs peuvent s'appuyer et qu'ils peuvent enrichir pour créer leurs propres contenus.

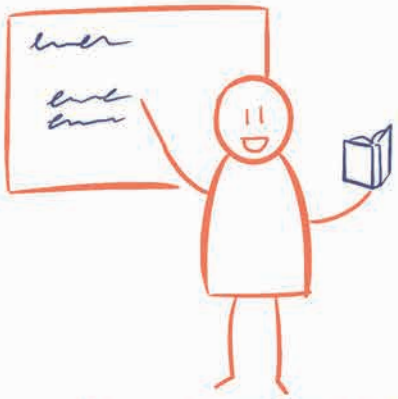
Matériel de création de jeux

Permettant de commencer à prototyper des jeux : dés, plateaux de jeux, pions, etc. Bien d'autres éléments peuvent par la suite compléter le kit, à partir d'objets courants, dans une logique de réusage ou bien achetés. Une vidéo présentant comment utiliser le kit est fournie à titre d'illustration.



Des prototypes de jeux numériques peuvent également être élaborés, grâce à des outils simples d'utilisation mentionnés à titre indicatif.

A qui ce kit est-il destiné ?



Aux enseignants

Souhaitant organiser, avec des élèves, une séquence pédagogique de création de jeux sérieux relatifs à la cybersécurité.

Aux administrations, collectivités, entreprises, associations, ...

Souhaitant organiser une séquence de création de jeux ou créer par elles-mêmes des jeux sérieux pour former ou sensibiliser à la cybersécurité.

Aux passionnés

Souhaitant créer seuls ou en équipe des jeux sérieux pour former ou sensibiliser à la cybersécurité, à destination des élèves ou d'autres publics.

Comment utiliser ce kit ?

Dans le cadre de l'organisation d'une séquence de création de jeux sérieux, le kit vous accompagne étape par étape.

Étape 1 : concevoir et préparer la séquence

Fiches organisation

Constituer l'équipe, fixer les objectifs, planifier, gérer la logistique...
Dérouler les différentes étapes de la séquence, faciliter les ateliers...

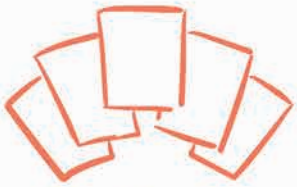
Fiches cybersécurité

Partager, si besoin, des connaissances aux participants en amont des ateliers
Transmettre certaines connaissances le jour J en guise d'inspiration, habiller l'espace...

Étape 2 : animer la séquence

Fiches jeux

Inspirer des types et modes de jeux.



Fiches objectifs pédagogiques

Orienter vers la création de jeux à destination des élèves, ...

Phase d'inspiration

Avoir tous les éléments en main pour être créatif.

Phase d'idéation et de prototypage des jeux

Imaginer les jeux et les prototyper.

Que faire des jeux créés ?

Vous avez organisé une séquence de création de jeux sérieux relatifs à la cybersécurité ?

Vous avez créé des jeux et les avez partagés en licence ouverte ?

Tenez-nous informés en écrivant à **lab-innov@ssi.gouv.fr** et **110bis@education.gouv.fr** !

Remerciements et informations relatives au partage du kit

Remerciements

Des enseignants et experts nous ont épaulés tout au long de la conception de ce kit et nous les en remercions ! Mention particulière à :

-**Laure Dousset**, fondatrice de Plush & Nuggets et gestion de projet sur ce kit Cyber en jeu.
-**Delphine Litchman**, enseignante de Sciences Economiques et Sociales chargée de l'enseignement des SNT dans le lycée polyvalent Marie-Louise Dissard dite Françoise à Tournefeuille (Académie de Toulouse).
-**Adrien Triboulet**, enseignant de mathématiques chargé de l'enseignement des SNT dans le lycée professionnel Château Blanc (Académie d'Orléans-Tours).
- **Alexandre Quach**, fondateur de la communauté Open Serious Games.
-**Les équipes de l'ANSSI et du ministère de l'Education nationale**, de la Jeunesse et des Sports.

Ce kit est un prototype

Pour rappel, ce kit à date de sortie (janvier 2021) est à l'état de prototype : les contenus qu'il contient sont des versions destinées à évoluer en fonction des retours utilisateurs. De ce fait, nous comptons précisément sur vous pour identifier des erreurs, pointer des incohérences, proposer des améliorations à réaliser, dans une logique contributive !

La licence de ce kit

FICHES «JEUX»

Ce que ces fiches vous permettent de faire et comment

Ces fiches visent à familiariser les organisateurs et participants d'une séquence de création de jeux sérieux avec les **différents types** et **modes de jeux.**

Sommaire

FICHE
Apprendre par les jeux sérieux

Un jeu sérieux, c'est quoi ?

D'abord, entendons-nous bien sur le terme de «jeu sérieux» : tel que défini par Julian Alvarez et Damien Djaouti en 2010 dans Introduction au Serious Game, il se caractérise par son «*intention initiale [...] de combiner, avec cohérence, à la fois des aspects utilitaires (Serious) tels, de manière non exhaustive et non-exclusive, l'enseignement, l'apprentissage, la communication, ou encore l'information, avec des ressorts ludiques issus du jeu vidéo (Game)*» ; aujourd'hui, le jeu sérieux adopte des formes plus variées, notamment inspirées des jeux de société, élargissant la définition «aux ressorts ludiques issus du jeu» en général.

Si le jeu a toujours été un outil d'apprentissage important notamment pour les jeunes enfants (interactions sociales, apprentissages visuo-spatial, dénombrement...), l'insistance sur le terme «sérieux» peut refléter à la fois une volonté d'élargir le public du jeu, souvent perçu comme réservé aux plus jeunes, et de le dédier à des sujets de fond complexes, utilitaires, peu attrayants...en bref, «sérieux».

Quels avantages d'apprentissage par le jeu sérieux ?

Ils sont nombreux mais à titre non exhaustif :

- Faire découvrir et encourager une appétence pour des thématiques a priori «sérieuses», ou faire voir un sujet sous une autre facette.

- Appréhender des notions du sujet présenté par le jeu de manière plus ou moins précise : connaissances théoriques (acteurs, rôles, connaissances relatives au fond) ou pratiques (mise en œuvre d'une méthode, d'une procédure...).

- Permettre l'interaction (avec un ordinateur, un ou plusieurs autres joueurs, un maître du jeu), ce qui favorise l'acquisition des connaissances et leur mise en œuvre si les mécaniques du jeu s'y prêtent.

- Faciliter l'implication du joueur-apprenant.

- Créer une expérience d'apprentissage qui sort de l'ordinaire, mémorable par son aspect social, la surprise du format...

FICHE
A quoi ressemble un jeu sérieux ?

Quels sont les différents types de jeux sérieux ?

Il existe de nombreux formats de jeux sérieux pouvant prendre appui sur des supports physiques (carton, papier, espace, etc.) et/ou numériques (application mobile, site internet, réseau social, etc.) ou bien les deux (hybrides). On peut notamment citer, parmi la liste immense des types de jeux sérieux existants : les jeux de plateau, tels que les jeux de conquête de territoire ou de construction ; les jeux de carte ; les Escape game ; les jeux de type «instructions» permettant la réalisation d'un exercice ou d'un défi ; les quizz, etc.

Ces jeux tirent, par ailleurs, partie de différentes mécaniques de jeux pouvant être combinées, à l'instar de :

- La **compétition** entre plusieurs personnes ou équipes, propice à la mise en situation d'intérêts contradictoires ou bien encore de forces et de faiblesses, pouvant se matérialiser sous forme de conflit, de négociation, de conquête, etc.

- La **coopération** selon laquelle les joueurs travaillent ensemble et non les uns contre les autres souvent afin de relever un défi commun pouvant prendre la forme d'une menace à éviter.

- Le **récit** faisant du jeu un cheminement, utile pour «guider» des joueurs dans la compréhension d'étapes, les responsabiliser en les invitant à faire des choix.

- Les **jeux de rôle**, invitant les participants à jouer des personnes ou fonctions précises, permettant notamment un changement de perspective des joueurs, en les obligeant à adopter un point de vue tiers.

- Le **défi** valorisant l'atteinte d'un objectif supérieur, par la résolution de problèmes ou en saisissant des opportunités. Le défi est propice à l'engagement des joueurs et à la mise en pratique des connaissances notamment s'il prend la forme d'une quête.

- L'**enquête** visant à lever un mystère, particulièrement adaptée lorsque le jeu vise à faire comprendre, par eux-mêmes, aux joueurs les sous-jacents d'un sujet, au-delà de ses apparences.

Les possibilités en termes de mécaniques de jeux sont infinies et largement documentées sur internet !

Quelques exemples de jeux sérieux

- **«Les Debriefing Cards»** : un petit jeu de cartes aux mécaniques très simples permettant de se poser les bonnes questions et de répartir la parole dans un groupe de travail afin que ce qui doit rester un court bilan ne devienne pas une conférence interminable !

- **«MineCraft4SCRUM»** : une adaptation du célèbre jeu vidéo Minecraft pour apprendre la méthode Scrum ! L'environnement et les mécaniques du jeu sont repris et adaptés pour mettre les participants en situation d'apprentissage de cette méthode agile.

- **«Codroid-19»** : un jeu de cartes coopératif créé pour mieux appréhender l'épidémie de Covid-19. Les mécaniques de jeux mettent en scène la manière dont le virus se propage, mais aussi les effets des différentes mesures qui peuvent être prises pour endiguer le phénomène, et permettent d'éprouver l'importance du facteur temps sur l'efficacité des mesures déployées.

- **«Foune et Flore»** : ce jeu de cartes fait le pari de faire acquérir des connaissances sur un sujet tabou et assez technique qu'est la microbiologie vaginale, et ce de manière ludique et attrayante. Il démontre que tout sujet peut faire l'objet d'un jeu agréable à jouer et qu'il n'y a aucun risque à s'y essayer !

- **«Expédition sagesse»** : pour répondre aux questions philosophiques tirées au hasard des cartes, les joueurs devront se concerter et argumenter ensemble de vive voix ! Cette interaction entre les joueurs, placée au coeur de la mécanique de jeu, permet de rassembler des profils très variés (enfants, adultes, publics débutants ou avertis...) avec convivialité.

- **«SCRUMind»** : ce jeu reprend la mécanique de Mille Bornes appliquée à la méthode agile Scrum. Cet exemple montre qu'il est possible de se mettre en situation et d'acquérir de bons réflexes sur un sujet d'experts, au moyen d'une mécanique de jeu connue de tous et facile à transformer !

Besoin d'autres exemples pour vous inspirer ? Retrouvez une liste de jeux sérieux sur le site de la communauté d'Open Serious Games **(https://openseriousgames.org/liste-des-openseriousgame/)** ou baladez-vous sur les nombreuses bases de référencement de jeux quil existent **(https://openseriousgames.org/trouver-des-serious-games/)** !

FICHES ORGANISATION

Ce que ces fiches vous permettent de faire et comment

Ces fiches constituent un guide clé en main d'organisation d'une séquence de création de jeux sérieux sur le thème de la cybersécurité. Vous y trouverez : des conseils pratiques sur la **logistique** à mettre en œuvre ou sur l'**animation** d'une séquence ; des ressources de fond à travers les «Fiches cybersécurité», incluant des fiches pédagogiques intégrées au **kit Cyber en Jeux**. Une fiche a spécialement été produite à destination des enseignants et des formateurs, afin de les aider à transformer une séquence de création de jeu en véritable séquence pédagogique, notamment dans le cadre de l'enseignement Sciences Numériques et Technologie (SNT).

Sommaire

FICHE
Concevoir une séquence de création de jeux sérieux

Pourquoi organiser une séquence de création de jeux sérieux ?

Pour former par la création de jeu : réaliser un jeu nécessite d'assimiler quelques éléments de fond avant de le mettre en forme ! Ainsi, les étapes de recherche du sujet du jeu, de collecte d'informations pour mieux l'appréhender, de réflexion autour de sa ludification et de création des supports constituent une phase d'apprentissage pour le créateur. Et cela de façon exploratoire et volontaire : l'un des avantages du jeu est d'impliquer fortement le(s) concepteur(s), qui investissent temps et compétences pour produire la meilleure version de leur idée ! En somme, ils se prennent eux-mêmes au jeu de faire un jeu.

Pour former par le jeu : jouer à un jeu peut être une entrée en matière décomplexée et amusante pour découvrir un sujet méconnu et/ou technique a priori ! Seul ou en groupe, lors d'une activité encadrée (formation, séance de classe, activité périscolaire...) ou sur son temps libre, le jeu est un moyen d'apprentissage extrêmement pratique : il offre au participant un espace sécurisé dans lequel il peut mobiliser ses connaissances, réitérer en cas d'erreur autant de fois qu'il le désire et progresser !

Les possibilités en termes de mécaniques de jeux sont infinies et largement documentées sur internet !

Les 4 étapes d'une séquence de création de jeux

Inspiration

En quoi cela consiste-t-il ? La phase d'inspiration a pour objectifs de :

- Communiquer des éléments de connaissance aux participants qui pourront se rafraîchir la mémoire ou permettre leur entrée en matière dans un sujet nouveau, en l'espèce la cybersécurité.

- Inspirer les participants, susciter de premières intuitions, ressentis, qui seront autant de ressources pour la création des jeux.

Les contenus en inspiration peuvent porter sur :

- Le fond (ici, la cybersécurité, complétée de quelques éléments théoriques relatifs aux mécaniques de jeu).

- La forme (des exemples de jeux, pas nécessairement en rapport avec le sujet de fond, ni même étiquetés «jeux sérieux»).

Pourquoi est-ce important ? Cette première phase est absolument nécessaire pour plusieurs raisons :

- En fournissant ce contenu initial à vos participants, vous vous assurez que tout le monde entre dans la prochaine phase, celle d'idéation, avec un socle commun : parce que vos participants ont tous des profils différents, chacun ne dispose pas nécessairement du même niveau de connaissances théoriques sur les différents aspects du sujet, il est donc impératif de fournir quelques bases qui faciliteront les échanges à venir.

- Les contenus que vous allez fournir vont orienter ce que les participants vont produire : prêtez une attention particulière à la qualité et à la variété des ressources que vous leur mettez à disposition, tant relatifs au fond qu'à la forme. N'hésitez pas à en jouer : si vous voulez que vos participants produisent des jeux très différents, montrez-leur des jeux de société, mais aussi des jeux vidéos, des jeux sur réseaux sociaux numériques, des livres-jeux... Au contraire, si vous voulez orienter la production uniquement sur des supports physiques, ne sélectionnez que des exemples allant dans ce sens.

Quelles en sont les modalités ? La phase d'inspiration peut prendre plusieurs formes :

- Lors d'un atelier, elle peut se matérialiser par une ou plusieurs présentations successives ou parallèles, sous la forme de «kiosques» thématiques chacun animé par une personne, auxquels les participants peuvent librement assister pour une durée limitée, sans nécessairement assister à tous.

- Sur une séquence plus longue, en particulier, dans le cadre d'une séquence pédagogique, l'inspiration peut être étalée dans la durée, sous la conduite, par exemple, d'un enseignant.

- La configuration et la décoration (affiches, messages, etc.) de l'espace où se tiendra la séquence d'inspiration peuvent également contribuer à faire naître des idées chez les participants.

Pour vous aider, retrouvez dans le kit...

Les «fiches cybersécurité», contenus de fond pour acculturer rapidement vos participants aux différents enjeux de la thématique !

Idéation et prototypage

En quoi cela consiste-t-il ? L'idéation désigne le moment où les participants vont imaginer différents concepts de jeux et décider, en groupe de travail, de celui qu'ils souhaitent développer, mais aussi des sujets qu'ils vont aborder et de la manière dont ils vont les traiter.

Une fois d'accord, ils passent à la conception du prototype de jeu (support du jeu, identité graphique, règles du jeu...).

Note : si votre séquence de création de jeux sérieux intègre des contraintes créatives (support ou type de jeu imposé, public cible précis...), elles doivent être communiquées aux participants dès le début de la phase d'idéation. Libre à vous d'en donner ou non !

Quelles en sont les modalités ? La phase d'idéation fait suite à la constitution d'équipes appelées à travailler en groupe. L'idéation n'a pas besoin d'être longue, le plus important étant de commencer à développer un jeu et à le tester, le faire évoluer.

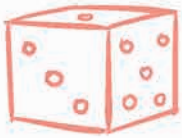
N'hésitez pas à venir en aide aux participants si vous constatez qu'ils patinent ; s'ils ont des difficultés à se décider, conseillez-leur de faire au plus simple et rapide, et de tester au plus vite leurs idées : c'est souvent en faisant que l'on constate ce qui fonctionne ou non. Bref, accordez autant de temps que possible à la phase de production ; votre animation permettra de rythmer cette dernière pour faciliter l'avancée des participants et les inciter à faire des choix.

Dès qu'un prototype semble viable, invitez l'équipe à le (faire) tester, ce qui leur permettra de le corriger et de l'améliorer, et ce autant que nécessaire et/ou que le temps de production le permet.

Pour vous aider, retrouvez dans le kit :

les cartes «objectifs pédagogiques» :

elles peuvent être utilisées, de manière facultative, pour aider à guider la création des jeux à destination des élèves. Vous pouvez, par exemple, faire choisir au hasard ou librement deux objectifs pédagogiques par équipe afin de restreindre le champ de l'idéation.



le matériel de conception de jeux :

vous pouvez aussi utiliser des fournitures/objets courants dans une logique de réusage ou bien acheter du matériel spécialisé.

Tests

En quoi cela consiste-t-il ? La phase de tests est, comme son nom l'indique, le moment de récolter des retours sur la jouabilité du prototype réalisé. Si les premiers tests peuvent être réalisés par l'équipe créatrice, il est impératif qu'elle le soumette à d'autres personnes extérieures à sa réflexion.

Pourquoi est-ce important ? Cette phase permet de s'assurer que les jeux réalisés sont bien jouables et que leurs règles sont suffisamment explicites pour être comprises par le public cible du jeu. Il n'est pas nécessaire que l'entièreté du jeu soit fonctionnelle ; un premier objectif atteignable de ces phases de production et de test peut consister en un segment cohérent.

Quelles en sont les modalités ? Les phases de tests interviennent dès qu'un prototype semble viable et lors de chaque ajustement fait sur le jeu suite aux commentaires des testeurs. Ces derniers peuvent être les organisateurs de l'événement, les autres participants, mais pourquoi pas un public extérieur à la séquence recruté à cette occasion (la famille des participants, des collègues d'un service voisin...).

Diffusion

En quoi cela consiste-t-il ? Cette ultime étape consiste en la mise au propre de la documentation du prototype, sur un support facilement diffusable (document pdf, diaporama, vidéo de présentation...). Soyez attentifs à ce que les participants vous fournissent tous les supports relatifs à leurs jeux : s'il manque quelque chose, il sera plus difficile de récupérer les pièces oubliées plus tard. Demandez également aux participants s'ils souhaitent être crédités à la création du prototype et sous quelle forme (pseudo, nom et fonction...).

Point d'attention concernant la licence de diffusion des jeux : il est important de communiquer en amont de l'événement et de rappeler lors de cette phase de diffusion que les jeux créés sont placés sous licence pour en assurer le partage. Nous vous conseillons l'utilisation de la licence Etalab, qui permet une diffusion ouverte, libre et gratuite autorisant la reproduction, la redistribution, l'adaptation et l'exploitation commerciale. Vous pouvez également opter pour une licence Creative Commons. Pour information, il n'est possible de protéger dans un jeu que les visuels et le nom de marque de ce dernier.

Quelles en sont les modalités ? Cette phase est souvent celle sacrifiée par manque de temps : elle est pourtant primordiale pour clôturer dans de bonnes conditions votre événement, et peut aisément tenir en 15mn. Afin de faciliter le processus, prévoyez un espace cloud sur lequel chacun viendra déposer sa documentation.

N'hésitez pas à communiquer les jeux sérieux que vous avez créés en lien avec la cybersécurité à **lab-innov@ssi.gouv.fr** et **110bis@education.gouv.fr** !

FICHE
Préparer la séquence

Choisir le format :
1 à 3 jours consécutifs ou étalé sur 1 à 2 semaines

1) Format resserré sur 1 à 3 jours consécutifs

La séquence peut prendre la forme conventionnelle d'un événement organisé sur une ou plusieurs journées entières consécutives (du type 9h-17h). La durée totale de la séquence variera en fonction du nombre de participants, de la complexité du fond et du degré de finition attendu des prototypes.

2) Format étalé sur une à deux semaines

Une alternative peut consister à segmenter les phases de la séquence pour les répartir sur un temps plus long, de 7 à 15 jours maximum. Un déroulé type d'une semaine peut s'organiser de la manière suivante :

Jour 1 : session d'une demie-journée maximum rassemblant tout le monde, pour lancer les phases d'inspiration et d'idéation en équipe,

Les 5 jours suivants, l'équipe réalise le prototype, par contribution individuelle et temps de concertation collectif (prévoir au minimum 1 heure de temps collectif par jour),

Jour 7 : session d'une demie-journée maximum où l'on rassemble tous les participants pour tester les jeux et les diffuser.

L'avantage d'une telle configuration est de mobiliser moins longtemps les participants sur des créneaux contraints, ce qui peut s'insérer plus facilement dans un agenda.

Se préparer concrètement : pas à pas

1) Monter une équipe de coordination

Cette équipe inclut l'équipe organisatrice, à l'origine de l'événement et associe les autres personnes ou services utiles à la réalisation de l'événement (communication, logistique, sécurité...).

2) Cadrer la séquence

L'équipe organisatrice détermine ensuite les éléments suivants :

-les objectifs de la séquence.
-le nombre et le profil des participant(e)s nécessaires, et en combien d'équipes ils seront répartis (entre 3 et 6 personnes maximum).
-la ou les date(s) de la séquence et les horaires.
-le déroulé minuté de la séquence.

3) Monter l'équipe de facilitation qui animera la séquence

Convenir de qui et combien de personnes facilitent la séquence, sont les personnes ressources de l'événement (graphisme, développement...), sont en charge du timing, font des photographies de l'événement, sont l'assistance technique en cas de besoin...

4) Identifier les partenaires de la séquence

Ce seront les personnes ou les contenus pour la phase d'inspiration, mais aussi des invités spéciaux, des entités partenaires éventuelles à convier, etc.

5) Inviter les participants et composer les équipes

Veillez à distribuer de façon homogène les compétences pour faire des équipes équilibrées.

6) Organiser la logistique

Pour un format en présentiel, il s'agira de réserver la ou les salle(s), de prévoir une éventuelle restauration, le matériel et les outils nécessaires, d'aménager et de décorer l'espace. Pour un format à distance, provoyez tous les outils utilisés pour communiquer avec les participants (visio-conférence en plénière et en sous-groupes, board en ligne, échanges asynchrones, partage de documents...), de les faire installer par les participants en amont de la séquence.

7) Après la séquence, valoriser les jeux créés

Pour en favoriser la diffusion, il s'agira de...

-Récolter tous les éléments qui constituent les prototypes des jeux (règles, supports de jeu, documentation éventuelle de la réflexion menée par le groupe...), pour vous aider sur ce point vous pouvez consulter les conseils prodigués par la communauté Open Serious Game sur comment transmettre un jeu,

-Les transformer en format numérique si besoin est (numériser les supports papiers, regrouper les éléments dans un même dossier avec des noms de fichiers explicites),

-Faire figurer la licence choisie (Etalab ou Creative Commons par exemple) sur les supports des jeux, dans une note explicative associée aux fichiers...

-Publier les jeux en ligne (site internet, GitHub, cloud partagé, base de référencement de serious games...)

Résumé de l'ensemble des rôles nécessaires au succès de la séquence

Une équipe organisatrice :

C'est elle qui recrute et informe les participants, qui veille à ce que tout soit prêt pour le(s) jour(s) J, qui gère le timing des différentes phases...

Les facilitateur(ice)s de la séquence :

Ce sont les personnes qui interviennent durant la séquence pour aider les participants à identifier et résoudre les problèmes, prendre des décisions et les engager dans la réalisation collective. Elles n'interviennent pas sur le fond et ne font pas les choix à la place des participants.

Les éventuel(le)s invité(e)s en inspiration :

Si vous avez dans vos contacts un expert en gamification, en cybersécurité ou en pédagogie, l'inviter pour une séquence d'inspiration d'un quart d'heure peut être très profitable à vos participants ! Son intervention doit éclairer les participants sur le(s) sujet(s) qu'ils maîtrisent le moins.

Les graphistes :

Nous vous recommandons de prévoir également le jour J des personnes en mesure d'aider les équipes sur le visuel de leur jeu s'ils ne disposent pas au sein de leur groupe de compétences graphiques. L'argument "je ne sais pas dessiner" est souvent un frein qui empêche les participants de se projeter dans la conception de leur jeu, qui peut être facilement désamorcé avec un coup de pouce graphique.
Ces personnes peuvent être des graphistes ou illustrateurs, mais aussi des professeurs d'arts plastiques, de technologie...

Les autres compétences rares :

En fonction de la nature des prototypes que vous voulez faire concevoir à vos participants et de leurs compétences, vous aurez peut-être besoin d'une ou plusieurs personnes ressources qui les aideront à concevoir leur prototype (développeur, concepteur de jeu...).

FICHE
Animer la séquence

Comment aider concrètement les équipes à faire un «bon jeu» ?

Une fois avoir dit qu' «un bon jeu est un jeu avec un objectif, des règles claires et sympa à jouer», on est pas très avancés...

Le but n'est pas de devenir un expert de la création de jeux qui est une compétence à part entière mais simplement de pouvoir aider les participants à se poser les bonnes questions lors de la création des jeux mais aussi à aider à formaliser ses retours éventuels sur un jeu !

Pour rappel, chaque règle ou élément du jeu doit :

-faire augmenter le plaisir de jouer et/ou,
-faire progresser les joueurs et/ou,
-obtenir les effets escomptés du jeu c'est-à-dire atteindre des objectifs pédagogiques et donc faire apprendre aux joueurs le contenu que l'on souhaite leur transmettre.

Ainsi, pour guider les équipes créatrices, vous pouvez en tant que facilitateur poser les questions suivantes lors d'un échange avec elles ou leur imprimer en guise de check-list :

-Vos règles du jeu sont-elles claires/explicites et complètes (rôles des joueurs, déroulement d'une partie...) ?
-Avez-vous indiqué les modalités pour jouer à votre jeu (combien de personnes, matériel à utiliser, temps de jeu...) ?
-Est-il clair de savoir par où commencer ?
-Comment gagne-t-on ? Comment perd-t-on ? d'ailleurs y a-t-il une victoire évidente ?
-Comment un joueur sait-il qu'il a gagné ? qu'il progresse ?
-Les joueurs ont-ils besoin de connaissances préalables, de pré-requis pour jouer à votre jeu ? Si oui lesquels ?

FICHE
Adapter en séquence pédagogique

Le cadre pédagogique

Vous êtes enseignant et souhaitez faire créer des jeux à vos élèves ? Cette fiche a été conçue pour vous faciliter la tâche !

Une séquence de création de jeux sérieux peut être envisagée dans le cadre de l'enseignement de Science Numérique et Technologie (SNT), afin de faire travailler les élèves de manière ludique sur les 7 objets du programme.

Cette modalité de travail avec les élèves participe à leur faire acquérir des compétences valorisées par le programme communiqué sur Eduscol, à savoir :

- savoir travailler en groupe,
- savoir travailler en autonomie en faisant preuve d'initiative et de créativité,
- concevoir une solution (créer un jeu sur le thème de la cybersécurité) à un problème (sensibiliser un public non-averti aux enjeux de cybersécurité),
- rechercher de l'information,
- acquérir des connaissances de fond,

...mais aussi potentiellement à les préparer à l'épreuve du grand oral par la présentation de leur travail devant l'ensemble de la classe !

Proposition d'une séquence sur 8 séances

Nous avons pris appui, pour la rédaction de cette fiche, sur le travail d'une enseignante de Sciences Économiques et Sociales de l'académie de Toulouse. La structuration proposée ci-dessous est directement tirée de sa séquence construite en 2020, accessible sur un support Genial.ly disponible à cette adresse à date de la rédaction du kit.

L'enseignante a construit sa séquence de manière à aborder dès le début de l'année scolaire tous les thèmes du programme en les décloisonnant. Le but : que les élèves aient une vision globale de celui-ci et qu'ils prennent connaissance une première fois des éléments clés de chacun des thèmes, avant de les revoir à l'occasion d'une séquence dédiée.

Pour les accompagner davantage et leur faire prendre du recul sur la conception de leur jeu, vous pouvez les amener à réfléchir au cadre d'utilisation de ce dernier :

- Indiquer 1, 2, 3 cas d'utilisations intéressantes de votre jeu,

- Au contraire, citez un exemple de cas où il ne faudrait pas utiliser votre jeu, même si cela semblait être à la base un bon cas de figure,

- Formuler en une phrase l'objectif de votre jeu,

- Choisissez trois verbes pour décrire le déroulement de votre jeu,

- Comment mieux capter l'attention du public cible de votre jeu ?

- Est-il possible de simplifier votre jeu : pour qu'il nécessite moins de pré-requis de la part des joueurs, pour qu'il demande moins de préparation avant de jouer, qu'il soit joué par un public moins expérimenté...

FICHE
Adapter en séquence pédagogique

Le cadre pédagogique

Vous êtes enseignant et souhaitez faire créer des jeux à vos élèves ? Cette fiche a été conçue pour vous faciliter la tâche !

Une séquence de création de jeux sérieux peut être envisagée dans le cadre de l'enseignement de Science Numérique et Technologie (SNT), afin de faire travailler les élèves de manière ludique sur les 7 objets du programme.

Cette modalité de travail avec les élèves participe à leur faire acquérir des compétences valorisées par le programme communiqué sur Eduscol, à savoir :

- savoir travailler en groupe,
- savoir travailler en autonomie en faisant preuve d'initiative et de créativité,
- concevoir une solution (créer un jeu sur le thème de la cybersécurité) à un problème (sensibiliser un public non-averti aux enjeux de cybersécurité),
- rechercher de l'information,
- acquérir des connaissances de fond,

...mais aussi potentiellement à les préparer à l'épreuve du grand oral par la présentation de leur travail devant l'ensemble de la classe !

Proposition d'une séquence sur 8 séances

Nous avons pris appui, pour la rédaction de cette fiche, sur le travail d'une enseignante de Sciences Économiques et Sociales de l'académie de Toulouse. La structuration proposée ci-dessous est directement tirée de sa séquence construite en 2020, accessible sur un support Genial.ly disponible à cette adresse à date de la rédaction du kit.

L'enseignante a construit sa séquence de manière à aborder dès le début de l'année scolaire tous les thèmes du programme en les décloisonnant. Le but : que les élèves aient une vision globale de celui-ci et qu'ils prennent connaissance une première fois des éléments clés de chacun des thèmes, avant de les revoir à l'occasion d'une séquence dédiée.

Séance 1 : introduction à la séquence

Il s'agit dans un premier temps de présenter aux élèves la séquence à venir (objectifs, organisation du temps de travail, les compétences transversales développées durant ce travail...). Ensuite l'enseignante leur propose un temps de discussion sur ce qu'est le game design : l'occasion de faire participer les élèves à l'oral, de redonner à tous des éléments sur le sujet et de commencer à leur donner des idées en leur présentant quelques types de jeux possibles dans ce contexte (voir séance 2). Enfin, l'enseignante balaie rapidement avec eux les 7 thématiques du programme et demande aux élèves de se constituer en groupe.

Modalités de constitution de groupes :

- 2 à 5 élèves par groupe : afin de développer leurs compétences de travail en équipe et permettre l'élaboration de prototypes de jeux plus complexes, l'enseignante a choisi de les faire travailler en groupe, en gardant une certaine souplesse dans la taille de ceux-ci, constitués par affinités,

- le choix a été fait de laisser les groupes choisir la thématique les inspirant le plus pour l'élaboration de leur jeu, quitte à ce que plusieurs groupes travaillent sur la même et que certaines ne soient pas représentées.

Séance 2 : réflexion sur le support de jeu

Les groupes sont constitués et les thèmes choisis : il s'agit maintenant de décider de la forme que prendra le jeu. L'enseignante segmente la réflexion collective en deux temps : d'abord elle présente les types de jeux possibles, puis redonne quelques indications concernant les mécaniques de jeu.

A- Les types de jeux

Ils peuvent être de nature très variés, et adopter des modalités physiques, virtuelles ou hybrides (voir les fiches "jeux").

Le jeu envisagé peut être soit un ensemble d'énigmes ou de défis décorrélés les uns des autres (comme par exemple un quizz en plusieurs parties), soit s'inscrire dans une même continuité (comme dans les jeux scénarisés de type escape game).

Afin de les inspirer, l'enseignant leur fournit à la fois des exemples d'outils en ligne sur lesquels créer leurs jeux, mais leur montre également des exemples de jeux réalisés à partir de ces mêmes outils. Lors de la discussion, les élèves sont invités à partager les jeux qu'ils connaissent et apprécient, et dont ils pourraient s'inspirer pour leur propre projet.

Note : le choix a été fait de laisser un maximum de possibilités aux élèves, mais l'on peut envisager de restreindre le type de productions à uniquement support matériel ou virtuel par exemple, pour homogénéiser les productions et les critères d'évaluation. Le matériel de prototypage fourni dans ce kit peut aussi servir de base à la production de ces jeux.

B- Points d'attention sur les mécaniques de jeu

Afin de guider les élèves et les aider à prioriser, l'enseignante leur redonne également des consignes relatives à la construction des mécaniques de jeu. Chaque règle ou élément du jeu doit :

- faire augmenter le plaisir de jouer et/ou,
- faire progresser les joueurs et/ou,
- obtenir les effets escomptés du jeu c'est-à-dire atteindre des objectifs pédagogiques et faire apprendre aux joueurs les repères historiques et autres informations contenues dans le jeu.

Dans le but de les guider, l'enseignante leur fournit une liste de questions qui les aideront à créer ces mécaniques de jeu :

- Vos règles du jeu sont-elles visibles et claires ?

- Est-il clair de savoir par où commencer ?

- Comment gagne-t-on ? Comment perd-t-on ? D'ailleurs, y a-t-il une victoire évidente ?

- Comment un joueur sait-il qu'il a gagné ? Qu'il progresse ?

- Pré-requis : les joueurs ont-ils tout ce qu'il faut pour répondre à vos défis ?

Enfin, l'enseignante leur présente les critères d'évaluation qu'elle compte appliquer au travail effectué (se référer au paragraphe «évaluation des travaux» pour consulter la grille d'évaluation proposée à cet effet).

A l'issue de cette présentation, les groupes travaillent ensemble et se mettent d'accord sur une première version de leur jeu. Lorsque leur idée est stabilisée, ils la soumettent à l'enseignante afin qu'elle valide le format de jeu choisi et la mécanique de jeu l'accompagnant.

Séances 3 à 6 : production du jeu

Les 4 séances suivantes sont dédiées à la réalisation du jeu en groupes. Les élèves avancent essentiellement durant le temps scolaire - charge à eux de s'organiser eux-mêmes s'ils veulent avancer hors du temps de classe s'ils en ressentent le besoin.

Les repères historiques de chaque thématique sont fournis par l'enseignante et chaque groupe approfondit sa connaissance du thème par des recherches personnelles. L'enseignante passe parmi les groupes afin de s'assurer de la bonne compréhension des éléments trouvés, de leur pertinence et de la fiabilité des sources sélectionnées.

Afin de faciliter la production des éléments du jeu par les élèves, l'enseignante leur propose des ressources en ligne pour...

- trouver des images ou icônes libres de droits,

- réaliser des cadenas virtuels, mais aussi des QR codes etc. en fonction des besoins des élèves.

C'est souvent en faisant que l'on se rend véritablement compte de si une idée fonctionne ou non ! Lors de ce temps de production, les élèves auront peut-être besoin de changer de concept de jeu car celui retenu ne se révèlera pas viable. D'autres concepts se trouveront, eux, être trop simples et demanderont complexification. Vous l'aurez donc compris, il faudra adapter les consignes à la production de chaque groupe et ne pas hésiter à réorienter ceux qui en ont besoin !

Enfin, lors de la 6ème séance, les élèves travaillent sur l'oral de présentation de leur jeu (cf séances 7 et 8).

Note : à titre d'information, sachez que cette séquence a été réalisée en début d'année scolaire, ainsi les élèves disposaient des vacances de la Toussaint pour finaliser leur jeu et peaufiner leur oral.

Séances 7 et 8 : passage à l'oral des groupes

Ces deux dernières séances visent à entendre la présentation de la production faite par chaque groupe.

Les modalités en étaient les suivantes :

- 10 min d'oral environ,

- présentation segmentée en deux parties :

  - un premier temps en groupe focalisé sur la présentation du jeu en tant que tel sous forme de«pitch»(environ 5 min) : présentation de l'équipe, de la démarche de création, explication du choix du format de jeu et de la mécanique l'accompagnant, présentation du thème sélectionné, et enfin mention des apports du projet et des compétences développées.

  - le second temps consiste en une prise de parole individuelle de chaque membre du groupe, qui doit expliquer : ce qu'il a apprécié ou non dans le projet, ce qu'il a appris, ce qu'il l'a surpris, ce qu'il a apporté au groupe et ce sur quoi il a contribué, et ce qu'il en retient pour plus tard.

Ce temps de présentation est idéalement suivi d'un moment de test du jeu par l'ensemble de la classe. En fonction du temps disponible, ce test peut être soit fait à la fin de chaque présentation, soit à l'issue de toute ou partie des passages où les élèves se répartissent sur les jeux, ou même hors du temps de classe si la possibilité d'une présentation des jeux lors d'un temps périscolaire est envisageable.

Note : il peut être intéressant d'avoir une trace écrite des jeux réalisés, que cela soit pour inspirer de futurs élèves sur la même séquence ou diffuser et valoriser plus largement les productions réalisées (à ce propos, n'hésitez pas à nous les partager à l'adresse **110bis@education.gouv.fr**). L'enseignante a envisagé deux solutions pour cela, à librement adapter :

- réalisation d'un mur collaboratif virtuel, permettant d'une part le suivi en temps réel de la progression des groupes et la sauvegarde des productions des élèves, voire pouvant servir de support pour la présentation orale des groupes,

- **OU** réalisation d'une affiche papier de présentation du jeu, à la manière d'une publicité et relistant les éléments essentiels du projet (auteurs, nom du jeu, slogan/concept, type de mécanique et supports de jeu...).

Evaluation des travaux

L'enseignante a fait le choix de noter ce travail afin d'évaluer notamment les compétences de prise de parole à l'oral des élèves, en vue de les entraîner à l'exercice du grand oral.

Afin de faciliter la notation, l'enseignante a conçu la grille d'évaluation suivante :

Évaluation groupe … : ……. / Thème : ……				
Évaluation du jeu, note de groupe	**/10**			
Qualité des informations recueillies	/5			
Présence des repères historiques et définition des notions du thème				
Qualité des recherches, fiabilité des sources, justesse des informations collectées				
Jouabilité du jeu	/3			
Le jeu est-il complet ? Jouable ?				
Les règles sont-elles claires, bien rédigées ?				
Originalité/créativité du jeu	/2			
Évaluation individuelle /10	Elève 1	Elève 2	Elève 3	Elève 4
Participation dans le travail de groupe lors des séances	/5	/5	/5	/5
Oral de présentation du jeu	/5	/5	/5	/5
Qualité de la prise de parole				
Aisance, fluidité, maîtrise du sujet				
Total	/10	/10	/10	/10
Note globale groupe + part individuelle	/20	/20	/20	/20

Informations complémentaires

Si le temps de travail nécessaire à la maturation d'une telle séquence est difficilement estimable, l'enseignante peut néanmoins quantifier les moments de réflexion et production suivants :

- création V1 du support communiqué en introduction de ce chapitre, qui regroupe l'ensemble des informations concernant la structuration de la séquence et les repères historiques de chaque thème : 4 heures consécutives. S'y ajoute les modifications apportées au fil de l'eau pour compléter au besoin.

- temps de suivi des groupes (essentiellement lors du temps de classe) et consultation des travaux à distance tant que de besoin.

- temps dédiés à l'évaluation, avec notamment test des jeux et relecture des supports produits.

Nous espérons que cet exemple de séquence pourra vous inspirer pour mener ce type de travail dans votre propre classe si la démarche vous intéresse !

Nous remercions chaleureusement Madame Litchman pour nous avoir donné la permission de présenter son travail, mais aussi pour sa contribution dans la relecture de ce chapitre.

Vous retrouverez ci-dessous, comme indiqué au début de ce chapitre, le support de présentation réalisée par l'enseignante et utilisé comme fil conducteur de la séquence.

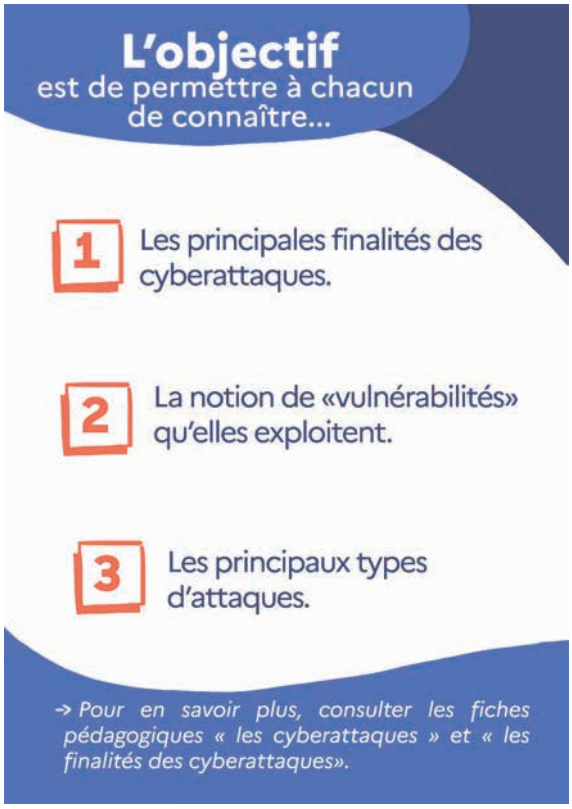
OBJECTIFS PÉDAGOGIQUES

Ce que ces cartes vous permettent de faire et comment

Les cartes "objectifs pédagogiques" explicitent les objectifs d'acquisition des connaissances par les élèves dans le cas de jeux sérieux créés à leur profit. Elles peuvent être mobilisées, sur une base facultative, en amorce de la phase d'idéation pour inviter les groupes à créer des jeux répondant à un ou plusieurs objectifs pédagogiques précis.

Connaître les sources de menaces

Connaître les cyberattaques et leurs finalités



Connaître les bonnes pratiques en matière de cybersécurité

Connaître les bonnes pratiques en matière de cybersécurité

Connaître

Les
cyberattaques
et leurs finalités

Connaître

Les sources
de menaces

Pratiquer

Le management
du risque

Connaître

Les
bonnes pratiques
en matière de
cybersécurité

Pratiquer la cryptographie

Comprendre l'environnement numérique & le cyberespace

Découvrir la détection & la récation aux cyberattaques

Découvrir la réglementation

Comprendre

L'environnement numérique & le Cyberspace

Pratiquer

La cryptographie

Découvrir

La règlementation

Découvrir

La détection & la réaction aux cyberattaques

Comprendre la cybersécurité

Découvrir les enjeux internationaux de la cybersécurité

Découvrir l'histoire de la cybersécurité

Découvrir

Les enjeux internationaux de la cybersécurité

Comprendre

La cybersécurité

Découvrir

L'histoire de la cybersécurité

FICHES CYBERSÉCURITÉ

Ce que ces fiches vous permettent de faire et comment

Ces fiches pédagogiques proposent des connaissances relatives à la cybersécurité, permettant de former les participants à une séquence de création de jeux sérieux. Ces fiches sont destinées à un public adulte, participant à une séquence de création de jeux sérieux ou préparant une séquence pédagogique impliquant des élèves.

Sommaire

Note : le contenu des fiches cybersécurité a été pensé pour simplifier et accélérer l'accès à des enjeux complexes relatifs à la cybersécurité. L'objectif est de permettre à des personnes n'ayant pas nécessairement de connaissances préalables du sujet de s'en saisir et d'être inspirées dans la création de jeux. Ces fiches ne sauraient donc être considérées comme expertes ou exhaustives.

Le cyberespace

L'essor du numérique, vers l'infini et au-delà !

Parler de cybersécurité, c'est d'abord s'intéresser à ce qu'il faut protéger dans l'espace numérique, composé de l'ensemble des équipements (téléphones, ordinateurs, tablettes), infrastructures informatiques et réseaux à l'échelle de la planète, également appelé « cyberespace ».

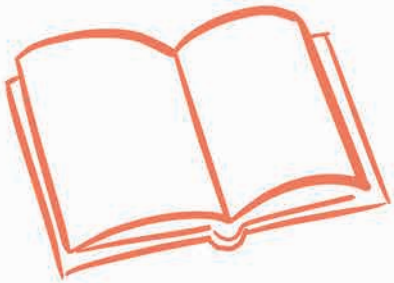
Depuis les années 60/70, l'émergence des premiers réseaux à des fins militaires ou de recherche (Arpanet aux Etats-Unis, Cyclades en France) a conduit à internet tel que nous le connaissons aujourd'hui. **L'essor du numérique a bouleversé le fonctionnement de la société et de l'économie, à l'échelle :**

- **D'un individu ou d'un foyer avec l'apparition des téléphones intelligents, ordinateurs, tablettes, etc.** Ces technologies permettent l'accès à la connaissance et à la culture, aux jeux, aux réseaux sociaux, aux films et séries, aux services publics en ligne, aux sites marchands, au Cloud et, de plus en plus, aux objets connectés (matériel sportif, balances, chauffage, etc.).

- **Des organisations et des entreprises, avec le passage au « tout numérique »** (postes de travail, processus internes, relations clients, méthodes de production et de distribution, etc.) **et l'émergence d'entreprises spécialisées dans le numérique** (Cloud, vidéo, jeu, etc.).

- **Des États, avec l'essor du numérique au sein de l'administration** et dans sa relation avec les citoyennes et les citoyens, grâce aux services publics en ligne. Cela passe **également par de nouvelles opportunités mais aussi la nécessité de faire face à de nouvelles menaces liées dans un « cyberespace »** mondialisé.

Le « cyberespace »



Imaginé par l'auteur de science-fiction William Gibson dans son livre « Neuromancien » (1983), le concept de « cyberespace » est aujourd'hui utilisé pour décrire l'ensemble des infrastructures, technologies et services numériques de par le monde, dont le principal : le réseau Internet.

Il possède également une dimension fortement géopolitique. Pour certains États, comme les États-Unis ou la France, le cyberespace est devenu un espace de confrontation à part entière pour les armées, à l'image d'autres espaces tels que la terre, la mer ou l'air.

D'un point de vue plus technique, le « cyberespace » est souvent représenté sous forme de couches.

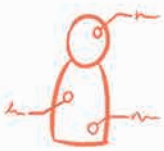
Une couche « matérielle »	Câbles et satellites connectant le monde à Internet, appareils (ordinateurs, téléphones, tablettes), clés USB.
Une couche « logicielle »	Systèmes d'exploitation permettant aux utilisateurs d'accéder aux fonctionnalités d'un ordinateur ou d'un téléphone, langages informatiques permettant de développer des applications (logiciels sur ordinateurs, applications mobiles, etc.).
Une couche « sémantique »	L'ensemble des informations, contenus générés, stockés, partagés : photos, vidéos, mails, etc.

Les systèmes et les données à protéger

Ce qu'il faut protéger

Se poser la question des systèmes d'information et des données qu'il faut protéger, c'est s'interroger sur leur valeur dans l'espace numérique.

On peut citer, par exemple :



- **Les données à caractère personnel** d'un individu (nom, prénom, adresse, numéro de téléphone, email, conversations privées, photos, données bancaires, etc.) dont l'utilisation à des fins malveillantes ou simplement de manière négligente expose à de nombreux risques : utilisation abusive de leurs données à des fins commerciales, atteinte à la réputation, fraude ou extorsion, usurpation d'identité, etc.

- **Les systèmes d'information des entreprises, petites ou grandes, ou encore d'organisations telles que des laboratoires de recherche. Ils détiennent de nombreuses informations sensibles,** essentielles au fonctionnement de ces entités (fichiers clients par exemple), mais également relatives à leurs produits, services, recherches et technologies. Ces derniers encourent de nombreux risques tels que l'inaccessibilité des informations, l'interruption partielle ou totale de service ou encore la compromission de secrets au profit d'un concurrent. Et à la clé, des pertes de chiffre d'affaire, des atteintes à la réputation...

- **Les systèmes d'information des opérateurs d'infrastructures critiques,** à savoir des entreprises publiques ou privées gérant des installations vitales pour le fonctionnement de la France ou des services essentiels pour l'économie et la société (gestion de l'eau, énergie, transports comme dans le secteur aérien, etc.).

- **Les informations classifiées** à savoir les informations les plus sensibles de l'État, dont la divulgation pourrait porter préjudice à la sécurité nationale.

Deux notions incontournables

Les systèmes d'information : A savoir l'ensemble des ressources permettant de traiter et de diffuser de l'information. Un ordinateur, un téléphone, une montre connectée, un serveur, le réseau interne d'un établissement scolaire comme le réseau mondial d'une entreprise sont donc des systèmes d'information. **Du concept de « systèmes d'information » découle celui de « sécurité des systèmes d'information », notion fondamentale dans le domaine de la cybersécurité.**

Les données : A savoir l'ensemble des informations numériques créées, traitées, stockées, sauvegardées, mais aussi accessibles, partageables, diffusables.

Un environnement numérique de plus en plus complexe

Deux tendances contribuent aujourd'hui à rendre le numérique plus complexe à appréhender... et à protéger :

- **La fin de l'époque où protéger un réseau informatique et les ordinateurs qui y étaient connectés nécessitait de sécuriser les entrées et sorties vers Internet du réseau d'une organisation, localisé dans ses locaux.** Avec le développement du travail à distance, l'interconnexion croissante des entreprises, etc. le numérique est devenu un immense écosystème interdépendant d'acteurs, de services, d'équipements. Cela est notamment rendu possible par le développement de l'informatique en nuage (Cloud) rendant accessible à distance de nombreux services et permettant l'accès à des données localisées à plusieurs endroits à la fois sur la planète.

- **La multiplication des acteurs impliqués dans la fourniture de matériel et de services numériques,** incluant de nombreux sous-traitants, fournisseurs ou intégrateurs, ayant tous un rôle à jouer dans la sécurisation des systèmes et des données.

La cybersécurité

Définition

La cybersécurité désigne l'ensemble des **activités** visant à protéger les **données** et **l'ensemble des « systèmes d'information »** contre les menaces issues du cyberespace susceptibles de compromettre leur **disponibilité**, leur intégrité ou leur **confidentialité**.

Disponibilité	Capacité à accéder à des données, services ou tout autre bien au moment souhaité. La disponibilité peut être, par exemple, compromise par la destruction (effacement de données par exemple), le chiffrement (il rend illisible les informations à moins de posséder la clé de déchiffrement) ou encore par l'interruption d'un service.
Intégrité	Propriété garantissant que des données ou tout autre bien sont exacts et complets et n'ont donc pas été modifiés. L'intégrité peut être, par exemple, compromise par la modification du contenu d'un fichier.
Confidentialité	Garantie que des données, des services ou tout autre bien ne sont accessibles qu'aux personnes autorisées. La confidentialité est compromise dès lors qu'une personne non autorisée accède à des données ou tout autre bien sans en avoir le droit.

Prévenir et répondre

La cybersécurité recouvre sur **deux dimensions principales** pouvant être appréhendées de manière chronologique soit avant, pendant ou après un incident informatique, qu'il soit dû ou non à une cyberattaque. De manière simplifiée on peut les rassembler en deux catégories.

La prévention (avant)	Cela correspond à l'ensemble des mesures permettant, autant que possible, à un système d'information de résister aux attaques ou vulnérabilités susceptibles de menacer les données et les services auquel il permet d'accéder. Ce volet renvoie schématiquement à la « sécurité des systèmes d'information ». La prévention passe notamment par : - Le management du risque, permettant d'identifier et de comprendre les principaux risques auxquels une organisation est exposée afin de déterminer quelles sont les mesures à mettre en place pour les prévenir. - Les mesures et moyens de protection technique des systèmes d'information, tels que le chiffrement. La mise en place de mesures non techniques telles que la sensibilisation des utilisateurs aux bonnes pratiques de sécurité informatique. - Le respect de règles techniques ou non par certains opérateurs dits critiques, tel que prévu par la loi.

La réaction (pendant et après)	L'ensemble des capacités permettant de détecter des cyberattaques et d'y répondre en vue de les stopper, de gérer, le cas échéant, une crise et de revenir à un mode de fonctionnement normal (résilience). La réaction aux cyberattaques passe notamment par : - La détection des cyberattaques. - La réponse à incident, par la mobilisation d'équipes techniques (les CSIRT). - La gestion d'une crise d'origine cyber au sein d'une organisation. - La reconstruction des systèmes d'information infectés. - La lutte contre les cybercriminels.

Acteurs de la cybersécurité

Assurer la cybersécurité des administrations, des citoyens et des entreprises est une tâche immense. Des acteurs publics et privés y travaillent d'arrache-pied 7 jours sur 7, 24h sur 24.

Outre les entreprises de cybersécurité, la sphère publique a un rôle essentiel à jouer en matière de protection.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI). Relevant des services du Premier ministre, l'ANSSI est l'autorité nationale en matière de cybersécurité.
Elle œuvre à la prévention des cyberattaques contre l'État, les opérateurs les plus critiques de la Nation et au-delà de l'ensemble de l'économie et de la société. Elle participe également à détecter et à répondre aux cyberattaques. Chaque année, l'ANSSI gère ainsi plusieurs crises cyber majeures, souvent en lien avec ses partenaires européens. Elle peut compter pour cela sur plusieurs centaines d'agents disposant d'une expertise technique, opérationnelle et stratégique de très haut niveau.

Le dispositif cybermalveillance.gouv.fr, est une plateforme d'assistance aux victimes d'actes cybermalveillants pour le grand public, les TPE/PME et les collectivités. Elle participe également à les sensibiliser aux menaces numériques.

Les sources de menace

Introduction à la menace cyber

La cybersécurité vise à garantir la sécurité des systèmes d'information et les données qu'ils contiennent contre des menaces informatiques ou « menace cyber » pouvant prendre la forme de cyberattaques, menées par des acteurs malveillants.

Cette menace d'origine cyber peut être perpétrée par un État, une organisation ou encore un individu indépendant. Celle-ci consiste à porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité des données présentes sur les systèmes d'information d'une victime en vue d'atteindre certains objectifs (gain financier, espionnage, déstabilisation, etc.).

Les quatre dimensions de la menace cyber

- **Un attaquant ou un groupe d'attaquants** aux profils divers.

- **Une cible** (personne, organisation, etc.) qui peut être le système d'information et/ou les données visées d'une victime.

- **Un objectif** qui correspond aux motivations de l'attaquant.

- **Un chemin d'attaque** ou un mode opératoire qui désigne les étapes et opérations que mène l'attaquant pour atteindre son objectif.

L'ado à capuche: le profil non-typique de l'attaquant!

L'attaquant cyber est souvent décrit à tort dans les films et les médias comme un « hacker » se résumant à un « jeune » isolé, portant un sweat à capuche et agissant tard dans la nuit pour « pirater la CIA » depuis l'ordinateur de sa chambre.

- Le terme « hacker » est, à tort, associé aux seuls acteurs malveillants. Pourtant, celui-ci renvoie historiquement à une culture positive de la « débrouille », du « partage » et de la « transformation » dans des domaines comme l'informatique mais également l'électronique, la menuiserie, la mécanique, etc. Par souci de distinction avec les acteurs malveillants, on parle désormais de « hackers éthiques ».

- Si l'attaquant isolé agissant depuis sa chambre constitue bien une catégorie réelle, celle-ci est caricaturale, négligeable en termes d'impact. Elle est surtout loin d'être la seule !

Les principaux profils d'attaquants en fonction de leurs motivations incluent :

	**Les amateurs, sans compétence particulière** (connus sous l'appellation « *script-kiddies* ») sont des attaquants disposant d'une faible expertise. Ils ont le plus souvent recours à des outils disponibles en « source ouverte » (par exemple sur internet) et facilement accessibles. **Leur motivation est ludique, récréative (« pour le fun »).**
	**Les attaquants « vengeurs » ou « malveillants »**, souvent isolés dont **la motivation est personnelle voire affective** (par exemple, une revanche contre un ex-employeur, un collègue ou un proche).
	**Les cyberhacktivistes** (fusion de hacker et activiste), soit tout type d'attaquant agissant selon **des motivations d'ordre idéologique, politique, etc.**
	**Les attaquants expérimentés dont la motivation est essentiellement technique.**
	**Les cybercriminels organisés et les mercenaires** travaillant à leur compte ou pour celui d'un particulier ou d'une autre organisation criminelle. **Leur motivation est principalement lucrative (financière).**
	**Les acteurs étatiques,** dotés de moyens souvent importants et aux **motivations multiples. Elles peuvent être de nature stratégique,** sont fonction des intérêts d'un État et peuvent parfois poursuivre un dessein offensif (mobilisation de moyens cyber dans le cadre d'un conflit armé ou à des fins de renseignement par exemple).

Les finalités des attaquants

Les finalités motivant les attaquants à réaliser des cyberattaques multiples.
On peut notamment citer les finalités suivantes :

	**Le défi, l'amusement,** visant à réaliser un exploit à des fins de reconnaissance sociale, de défi ou de simple amusement. Même si l'objectif est essentiellement ludique et sans volonté particulière de nuire, ce type d'opération peut avoir de lourdes conséquences pour la victime.
	**L'espionnage** a pour objectif l'exfiltration d'informations stratégiques, de secrets de fabrication ou encore de données R&D détenus par des secteurs stratégiques de l'économie ou par l'État.
	**L'influence, l'agitation** consistant à agir sur le champ de l'information, souvent à l'initiative de cyberhacktivistes : détournement de comptes sur les réseaux sociaux, défiguration de site internet, etc.
	**La cybercriminalité à des fins lucratives** désigne principalement les attaques visant à retirer un pécuniaire d'activités cyber malveillantes. Il peut s'agir du recueil illicite de coordonnées bancaires, d'une cyberattaque à l'encontre de systèmes bancaires et financiers, etc.
	**Le pré-positionnement stratégique** consiste à se positionner discrètement dans un réseau informatique sans volonté d'agir immédiatement, par exemple pour préparer une attaque future, sans que la finalité poursuivie soit toujours évidente.
	**L'entrave au fonctionnement, par des opérations de sabotage, de neutralisation** désigne les attaques dont l'objectif est de rendre indisponible un système d'information et des données, par la saturation (ex : attaques par « déni de service » pouvant rendre inaccessible un site Internet ou encore les « rançongiciels ») voire par la destruction physique de matériel (ex : tromper des instruments de mesure dans les installations d'un opérateur d'infrastructure critique afin d'empêcher les mécanismes d'alarme de se déclencher et aller jusqu'à la destruction du système).

Les cyberattaques

Quelques exemples d'attaques

Les cyberattaques de type rançongiciel (*ransomware en anglais*), contraction des mots « rançon » et « logiciel » est une cyberattaque consistant à installer un programme malveillant, si possible sur le maximum d'équipements du système d'information de la victime, dans le but d'obtenir de celle-ci le paiement d'une rançon. Pour y parvenir, le rançongiciel va empêcher les utilisateurs d'accéder à leurs données (photos, fichier client, etc).

Les attaques par déni de service (*denial of service en anglais*) visent à rendre indisponible un ou plusieurs services. Pour ce faire, un nombre trop important de requêtes peut être adressé au dit service (site web, service de résolution de noms, etc.), le rendant inaccessible à d'autres utilisateurs. On parle de déni de service distribué (*destributed denial of service ou DDoS*) lorsque l'attaque prend appui sur un réseau de machines « zombies » préalablement manipulées à l'insu de leur prioritaire. Ces réseaux peuvent être composés de serveurs, d'ordinateurs ou encore d'objets connectés à Internet comme des caméras de vidéos surveillance. Lorsqu'ils sont composés de machines compromises on parle « botnets ».

Les cyberattaques persistantes (*Advance Persistent Threat en anglais*) (ou **APT**) sont des attaques plus *sophistiquées*, à la portée d'acteurs malveillants disposant de compétences et/ou de ressources leur permettant de pénétrer en profondeur dans un réseau. Ces attaques sont principalement menées à des fins d'espionnage économique, industriel ou scientifique.

Les vecteurs d'attaques

Humain 	Les personnes sont les premiers vecteurs d'attaque. En ayant recours à des techniques dites « d'ingénierie sociale », les attaquants peuvent par exemple avoir recours au hameçonnage (*ou phishing*) pour tromper la vigilance de leur cible (voir ci-dessous les « grands types d'attaques »). Une autre manière de procéder peut être de laisser traîner des clés USB infectées par un code malveillant, en pariant sur le fait que des salariés négligents les ramassent et les connectent au réseau de l'organisation.
Informatique 	Les techniques informatiques et codes malveillants permettant de nuire à un système informatique ou à un réseau sont un autre vecteur d'attaque.
Physique 	S'introduire dans une pièce (salle serveur ou bureau par exemple), sectionner des câbles, voler un serveur etc. sont autant d'autres moyens physiques permettant d'accéder à un système d'information ou de l'endommager.

Les vulnérabilités

Les cyberattaques exploitent des vulnérabilités, soit **une ou plusieurs failles repérées dans un système.**

En matière de cybersécurité, l'enjeu est de les identifier et de les corriger. Ces vulnérabilités peuvent être de nature :

- **Technique** au sein d'un équipement ou du code d'un logiciel, présente par négligence ou introduite dès la conception de manière involontaire. Elles peuvent être corrigées par la mise en œuvre d'un correctif de sécurité.

- **Organisationnelle** : absence de sensibilisation des utilisateurs, absence de prise en compte du risque cyber.

Les mesures de protection

L'hygiène informatique

Des mesures de protection techniques et non techniques (ex. sensibilisation, mise en place d'une organisation de gestion du risque cyber) sont nécessaires en vue de prévenir les cyberattaques et de se préparer à y répondre.

Parmi les nombreuses mesures susceptibles d'être mises en œuvre, certaines sont communes à toutes et à tous. On parle de « mesures d'hygiène cyber » :

- Pour les particuliers (voir les bonnes pratiques recommandées sur la plateforme cybermalveillance.gouv.fr).

- Pour les petites et moyennes entreprises (TPE/PME) (voir le guide pour co-édité par l'ANSSI et la CGPME intitulé GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE 12 règles essentielles pour sécuriser vos équipements numériques).

- Pour les organisations de taille plus importante (voir le guide des 42 mesures édité par l'ANSSI).

En complément de ces mesures et des règles, parfois imposées par la loi aux opérateurs les plus critiques, une démarche de management des risques est également nécessaire pour se protéger des risques stratégiques.

Quelques mesures incontournables

1. Bien gérer ses mots de passe : utiliser des mots de passe, y compris pour l'accès un téléphone ou un ordinateur et bien les choisir (voir les recommandations pour bien choisir son mot de passe sur cybermalveillance.gouv.fr). Autant que possible, utiliser un gestionnaire de mots de passe de confiance et dès que possible mettre en place des sécurité additionnelles pour accéder aux comptes (mails, réseaux sociaux) comme la « double authentification » (impliquant deux vérifications consécutives avant de permettre l'accès à un service), afin d'éviter que quelqu'un n'en ayant pas l'autorisation y accèdent.

2. N'utiliser que des logiciels officiels et à jour (par exemple issus des bibliothèques d'application mobiles officielles) et mettre à jour ces logiciels (système d'exploitation d'un ordinateur, logiciels de bureautique, applications mobiles).

3. Effectuer des sauvegardes régulières de ses données pour pouvoir les récupérer, dans le cas où ces dernières seraient détruites ou rendues inaccessibles.

4. Utiliser des réseaux wifi sécurisés sécurisés en évitant les réseaux sans mot de passe et sécuriser l'accès wifi d'un foyer ou d'une entreprise.

5. Être aussi prudent avec un smartphone et une tablette qu'avec un ordinateur et bien séparer les usages personnels et professionnels.

6. Être vigilant lors d'un paiement sur Internet.

7. Prendre soin de ses informations personnelles, professionnelles, de son identité numérique. Penser notamment à chiffrer les données – la plupart des ordinateurs permettent de chiffrer le disque dur – à savoir les rendre illisibles à qui y auraient accès mais ne sauraient pas les « déchiffrer ».

La cryptographie

Chiffrer pour protéger

La cryptographie est l'ensemble des procédés permettant la transformation d'un message en « clair » – c'est-à-dire compréhensible par n'importe qui y ayant accès – … en un message « chiffré », compréhensible seulement de celles et ceux disposant d'une « clé » pour le déchiffrement (une clé de déchiffrement). Les messages sont chiffrés grâce à des algorithmes de chiffrement, soit des suites mathématiques.

Grâce à ce procédé, deux personnes peuvent échanger de manière confidentielle et sécurisée, pourvu qu'elles possèdent toutes deux la clé leur permettant de chiffrer et de déchiffrer leurs messages.

La cryptographie est l'un des piliers historiques de la cybersécurité. Elle permet notamment de protéger les informations les plus sensibles de l'État, des entreprises, des centres de recherche. Le chiffrement peut également servir à protéger la confidentialité des données à caractère personnel des particuliers.

Exemple

Bob et Alice sont en classe. Ils n'ont plus leur téléphone portable et veulent s'envoyer un message sans que personne ne puisse le lire. Bob « chiffre » son message grâce au code CESAR (voir ci-dessous) et le transmet en le faisant passer de main en main jusqu'à Alice. Alice est au courant de la façon dont Bob a chiffré son message et parvient à le déchiffrer!

Message d'origine en clair

On mange ensemble ce midi ?

De nombreux sites internet en ligne permettent de s'exercer simplement s'exercer au chiffrement et au déchiffrement de messages.

Méthode de chiffrement

CESAR avec un décalage de 3 lettres dans l'alphabet.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

=

DEFGHIJKLMNOPQRSTUVWXYZABC

Message chiffré

Rq pdqjh hqvhpeoh fh plgl ?

Note : Bob et Alice sont deux personnages classiques utilisés dans le domaine de la cryptologie.

On dit, on ne dit pas !

On dit : chiffrement, chiffrer, déchiffrer... et **décrypter,** lorsque l'on cherche à accéder, par des moyens de cryptanalyse, à une information chiffrée sans disposer de la clé de déchiffrement (comme entrer dans une maison sans la clé).

On ne dit pas : cryptage, encodage, crypter, code, encoder... ni décrypter lorsqu'on a la clé de déchiffrement ! En savoir plus sur **https://chiffrer.info/**

scan me

Cryptologie, cryptanalyse, cryptographie : quelles différences ?

La **cryptologie** est étymologiquement la science du secret. Elle comporte 2 branches :

- La **cryptographie**, décrite précédemment.

- La **cryptanalyse**, est l'étude de systèmes cryptographiques permettant de chiffrer des données afin d'en évaluer la robustesse (par la recherche de failles tentatives de lecture des données chiffrées par exemple) lorsque l'on ne dispose pas de la clé de déchiffrement.

Une brève histoire de codes

- 50 avant JC : Le chiffre de César est l'un des chiffres de substitution que Jules César (100-44 av. J.-C.) avait coutume d'employer dans ses récits et correspondances. Il consiste à substituer une lettre par une autre en décalant l'alphabet de trois places vers la droite.

Message d'origine	B	O	N	J	O	U	R
Numéro de la lettre dans l'Alphabet	2	15	17	10	15	21	18
Numéro augmenté de 3	5	18	20	13	18	24	21
Lettres correspondantes	E	R	Q	M	R	X	U

- Au XVIe siècle : le diplomate français Blaise Vigenère invente une nouvelle méthode de chiffrement, le chiffre de Vigenère. Il est beaucoup plus solide que, par exemple, le chiffre de César : on n'a trouvé le moyen de casser cette méthode qu'en 1863 ! Elle est donc restée efficace pendant trois siècles !

- 1975 – 2000 : Le Data Encryption Standard **(DES)** est un algorithme de chiffrement symétrique standardisé en 1976. Il utilisait alors une clé de chiffrement de 56 bits, jugée à l'époque suffisante pour prémunir les entreprises du risque d'espionnage industriel, ce qui n'est plus le cas aujourd'hui. En 2000, DES cède la place à l'algorithme Advanced Encryption Standard **(AES)**, encore en usage aujourd'hui et dont les propriétés, parmi lesquelles des clés d'au moins 128 bits, offrent un niveau de sécurité bien plus grand.

Le management de risque

Part.1

Pourquoi gérer les risques cyber ?

Face à l'ampleur et la diversité des menaces susceptibles d'émaner du cyberespace, une organisation ou un État ne peut pas tout protéger contre tout, tout le temps.

En complément des mesures parfois rendues obligatoires par la loi et des bonnes pratiques de sécurité informatique communes à toutes les organisations (entreprise, association, administration) et aux particuliers, **analyser les risques principaux auxquels est exposée une organisation, c'est choisir les risques contre lesquels se protéger en particulier.**

Comment manager les risques cyber ?

La méthode EBIOS Risk Manager, développée par l'agence nationale de la sécurité des systèmes d'information (ANSSI), fournit les clés pour mettre en place une démarche de « management du risque cyber » pour les responsables d'une organisation (administration, établissement public, entreprise, association). Ses étapes majeures sont décrites ci-après :

Étape 1 - Cadrage

L'organisation doit tout d'abord identifier ce qu'elle tient à protéger (« valeurs métiers ») et les évènements redoutés, leurs impacts, leur gravité (sur le plan du fonctionnement de l'organisation, matériel, humain, financier, environnemental).

Exemple fictif pour un établissement scolaire de données ou services importants :

- Les notes et les données personnelles des élèves.
- La gestion des emplois du temps.
- Les accès internet de l'établissement, y compris pour les élèves.

Exemple fictif d'évènements redoutés et leur impact :

- L'intégralité des notes est supprimée ou quelques notes sont modifiées (à la hausse ou à la baisse).
- Les emplois du temps et les numéros de salle de classe modifiés plusieurs fois qui empêcheraient ou perturberaient la tenue des cours.
- L'ensemble des ordinateurs bloqués, rendant impossible la réalisation de certains cours nécessitant du matériel informatique, les fonctions administratives sont incapables de travailler.

Étape 2 – Sources de risques

L'organisation doit se poser la question de qui ou quoi pourrait porter atteinte aux missions et aux valeurs métiers de l'organisation et dans quel but.
En résumé : qui ou quoi pourrait vouloir me porter préjudice ?

Exemple fictif pour un établissement :

- Des cybercriminels cherchant à s'enrichir, diffusant aléatoirement sur internet des logiciels malveillants ne ciblant pas l'établissement, mais parvenant à l'infecter par hasard.
- Des élèves souhaitant simplement essayer, pour la technique, pour s'amuser à perturber l'informatique de l'établissement.
- Des élèves souhaitant améliorer leur note ou baisser les notes d'autres élèves.

Étape 3 – Scénarios stratégiques

L'organisation cartographie son écosystème numérique interne mais aussi externe, notamment ses « parties prenantes critiques » – fournisseurs d'équipements, de services, sous-traitants, clients – par lesquels une source de risque est susceptible de passer pour lui porter atteinte. Elle identifie ensuite des scénarios d'attaques de haut niveau ou « stratégiques ».

Exemple fictif pour un établissement :

- Les élèves ou le personnel de l'établissement accédant à internet infectent, par mégarde, un ou plusieurs ordinateurs de l'établissement (ex. en cliquant sur une pièce jointe infectée ou en allant sur un site infecté).
- L'un des services numériques en ligne (ex. plateforme pédagogique) utilisé par l'établissement comporte une vulnérabilité utilisée par des attaquants qui obtiennent accès aux données d'organisations utilisant ces services, dont celles de l'établissement.
- Un prestataire de maintenance informatique est attaqué pour parvenir à atteindre, dans un second temps, l'établissement.

Le management de risque

Part.2

Étape 4 – Scénarios opérationnels

L'organisation cherche ensuite à identifier les scénarios techniques (modes opératoires d'attaques) susceptibles d'être utilisés par les sources de risques pour réaliser les scénarios stratégiques.

Exemple fictif pour un établissement :

- Une pièce jointe piégée est ouverte en accédant à son interface mail professionnelle ou personnelle depuis un poste informatique de l'établissement.

- Une clé USB infectée à son insu, est introduite par l'un des prestataires de l'établissement. Un attaquant infecte un site Internet de l'établissement (ex ; le site des emplois du temps) afin d'infecter les machines des élèves et enseignants qui le visitent (attaque dite par « point d'eau »).

Étape 5 – Traitement du risque

Cette dernière étape vise à faire la synthèse des principaux risques et de définir une stratégie de traitement de ces derniers. Cela signifie notamment choisir quels risques traiter en priorité (souvent en fonction de leur gravité et de la probabilité de leur survenue)... et les risques que l'on accepte de prendre (risques résiduels). La stratégie de traitement des risques conduit ensuite à fixer les mesures de sécurité à mettre en œuvre de manière continue.

Détecter les cyberattaques

La détection

Réagir face à une cyberattaque suppose de... savoir qu'une attaque est bien en train de se dérouler. Et rien n'est moins simple, tant les attaquants peuvent se faire discrets et les attaques ne pas causer de dommages visibles.

Pour cela, la « détection des cyberattaques » est une activité clé de la cybersécurité. Elle repose sur des dispositifs techniques, en particulier les « sondes de détection » permettant de détecter des « signatures d'attaques » à savoir des traces de cyberattaques déjà rencontrées par le passé ou des comportements anormaux, par exemple, un ordinateur utilisé un dimanche alors que les locaux d'une entreprise sont fermés...

L'existence d'un dispositif de détection ne garantit pas de tout voir et peut même parfois se tromper. On distingue :

- les « faux positifs » correspondent à des activités légitimes détectées comme malveillantes.
- les « faux négatifs » correspondent à des activités malveillantes détectées comme... légitimes.

L'avantage aux attaquants

La difficulté à détecter les attaques et les attaquants est d'autant plus complexe qu'existe une asymétrie entre les attaquants et les personnes en charge de la cybersécurité, à l'avantage des premiers. Plusieurs raisons concourent à cela :

- **Une attaque informatique n'est pas en soi « visible »** à moins que les conséquences de l'attaque le soient (ex. destruction de données, sabotage) ou que les attaquants ne soient pas discrets par incompétence. Cette « discrétion » des attaques joue en faveur des attaquants.
- **Les outils et techniques mobilisables par les attaquants sont très nombreuses et parfois inconnues des défenseurs**. Les attaquants peuvent, par exemple, exploiter des vulnérabilités de systèmes d'information non encore connues (vulnérabilités dites « 0-day »).
- **Le cyberespace mondialisé permet aux acteurs malveillants d'attaquer des systèmes depuis l'autre bout de la planète.** On parle d'« ubiquité ». Trouver et poursuivre les attaquants en est d'autant plus complexe.
- **Le coût d'une cyberattaque peut être très faible et les capacités techniques nécessaires très accessibles** en comparaison des dommages susceptibles d'être causés. Ces propriétés facilitent l'activité de « cyberattaquant ».

Tenter de tout protéger, tout le temps, contre des attaquants discrets et des attaques souvent invisibles, agissant avec une boîte à outils potentiellement infinie... tel est le défi des acteurs de la cybersécurité !

Réagir aux cyberattaques

Répondre à un incident informatique

Lorsqu'une attaque informatique est détectée, l'objectif pour une organisation victime est de la faire cesser, limiter ses impacts et revenir à la normale.

Pour cela, plusieurs étapes seront franchies :

- Comprendre et caractériser l'attaque et les impacts causés ou susceptibles d'être causés.
- Contenir et protéger les systèmes concernés.
- Faire cesser l'attaque, en désinfectant/réparant, puis en restaurant et en reconstruisant les systèmes concernés.

Acteurs principaux de la réponse à incident les équipes de réponse à incident de sécurité – les CSIRT (*computer security incident response team)* ou CERT – sont les « médecins » chargés d'intervenir et de diagnostiquer les mesures à prendre pour faire cesser l'infection. Ils sont aussi souvent les « pompiers » qui interviennent eux-mêmes pour éteindre l'incendie. Le CSIRT d'une organisation peut également coopérer avec d'autres équipes en-dehors d'une organisation, en France et à l'international.

La gestion d'une crise d'origine cyber

On parle de crise « d'origine cyber » face à un incident informatique malveillant brutal, soudant, menaçant gravement la stabilité d'une organisation, d'un ou plusieurs États :

- Pour une ou plusieurs organisations, comme l'interruption de la fourniture d'un service à des clients ou la divulgation de leurs données à caractère personnel... source d'un mécontentement légitime.
- Pour la France voire l'Europe, lorsque les conséquences d'une cyberattaque s'avèrent massives, par le nombre de victimes ou les impacts causés par l'attaque (ex. interruption de la fourniture de services essentiels comme l'électricité ou l'accès à internet).

Face à une telle crise, la réaction d'une organisation ou d'un État ne pourra pas être seulement technique mais également opérationnelle et stratégique (coordination interne, avec les partenaires, communication, etc.) afin de permettre une sortie de crise rapide.

A l'échelle de l'État français, existent des dispositifs de gestion des crises de toutes origines, notamment cyber :

- Le Premier ministre prépare et coordonne au niveau politique l'action des pouvoirs publics en cas de crise majeur (art. L. 1131-1 du code de la defense).

- La cellule interministérielle de crise (CICI), activée par le Premier ministre, met en œuvre la réponse globale de l'État. Elle réunit des représentants de haut niveau des différents ministères concernés et autres entités comme l'agence nationale de la sécurité de système d'information (ANSSI), dans le cas d'une crise d'origine cyber.

- Des plans préexistent à certains types de crise afin de préparer la prise de décision des autorités. Le plan spécifique au cyber s'appelle Piranet mais le cyber fait désormais parti d'autres plans de gestion de crise.

- La gestion de crise de l'Etat français nécessite, par ailleurs, la conduite régulière d'exercices de gestion de crise.

Les règles en matière de cybersécurité et de lutte contre la cybercriminalité

Des catégories de règles existent en matière de cybersécurité et de lutte contre la cybercriminalité :

Les règles visant à renforcer la protection des systèmes d'information de l'administration et d'opérateurs particulièrement critiques, en les obligeant à mettre en œuvre certaines mesures techniques et non techniques pour protéger leurs systèmes d'information.

Les règles visant à prohiber et, le cas échéant, punir des actions ou comportements dommageables en ligne.

Les règles pour renforcer la cybersécurité

2 familles de réglementation participent particulièrement au renforcement de la cybersécurité en France

- **Les règles s'appliquant aux administrations** afin de garantir un niveau de sécurité adapté de ses systèmes d'information et des services publics numériques notamment accessibles au public. Ces règles incluent la politique de sécurité des systèmes d'information de l'État (PSSIE) ou encore le règlement général de sécurité (RGS).

- **Les règles applicables aux opérateurs publics et privés les plus critiques.** Cela inclue les « opérateurs d'importance vitale » (loi de programmation militaire de 2013) gérant des installations indispensables à la survie de la Nation et les règles européennes applicables aux « opérateurs de services essentiels » pour l'économie et la société. Critiques, ces opérateurs doivent mettre en œuvre des mesures de sécurité numérique et notifier à l'autorité nationale de cybersécurité (l'agence nationale de la sécurité des systèmes d'information, ANSSI), les incidents survenus sur leurs systèmes d'information.

- **Les règles applicables à l'ensemble des entreprises, administrations, associations en vue de protéger les données à caractère personnel.** La loi informatique et libertés en France et le règlement européen sur la protection des données à caractère personnel dit « RGPD » imposent à toutes ces entités de prendre des mesures afin d'assurer la sécurité de ces données, comme le chiffrement.

Les amendes et peines de prison pour des actions ou comportements illicites en ligne

Le droit français, en particulier le code pénal, prévoit plusieurs infractions pouvant entraîner des amendes et peines de prison, lorsqu'elles ont été commises en ligne :

-**L'escroquerie** *(article 313-1 du code penal),* passible d'une peine d'emprisonnement de cinq ans et de 375000 euros d'amende

- **La collecte de données a caractère personnel par un moyen frauduleux, déloyal ou illicite** *(article 226-18 du code pénal)* : une telle collecte constitue un délit passible d'une peine d'emprisonnement de cinq ans et de 300 000 euros d'amende.

- **Les acces, entraves, extraction de données, et autres comportements frauduleux envers un système de traitement automatise de données** *(article 323-1 et suivants du code penal)* comme un ordinateur, un serveur, téléphone, ou tout autre système d'information. Les peines peuvent atteindre sept ans d'emprisonnement et 300.000 euros d'amende. La tentative est réprimée de la même manière. Le fait de posséder des outils permettant de réaliser ces infractions, même sans en faire usage, est également illégal (323-3-1).

- **La contrefaçon et l'usage frauduleux de moyen de paiement** *(articles L. 163-3 et suivants du code monetaire et financier)* : delit passible d'une peine d'emprisonnement de sept ans et de 750000 euros d'amende.

- **L'usurpation d'identite d'une personne tierce** *(article 226-4-1 du code penal),* passible d'une peine d'un an d'emprisonnement et de 15000 euros d'amende.

- **La contrefacon des éléments visuels (logos, signes, identité graphique, emblemes...) utilises lors de l'hameconnage** *(articles L. 335-2 et suivants et L. 716-10 et suivants du code de la propriete intellectuelle)* : Delit passible d'une peine d'emprisonnement de trois ans et de 300000 euros d'amende.

Paix, sécurité, stabilité du cyberespace

Le cyberespace, source croissante de conflictualité

Désormais considéré comme un espace de confrontation à part entière par les armées de plusieurs États dans le monde, le cyberespace est devenu le lieu de rapports de force entre États mais également entre États et acteurs non-étatiques (cybercriminels, terroristes, etc.).

Si l'utilisation de capacités cyber-offensives par des États dans le cadre de conflits armés régis par le droit international public vient simplement s'ajouter à l'arsenal des capacités conventionnelles à la disposition des armées, l'utilisation de ces moyens en-dehors de ce cadre suscite un risque nouveau : celui qu'une crise d'origine cyber conduise à un conflit entre États, notamment dans le monde physique.

Renforcer la confiance entre États

Que cela soit entre États partenaires ou États n'ayant pas d'autre intérêt partagé que d'éviter un conflit, plusieurs mécanismes concourent à renforcer la sécurité et la stabilité internationale du cyberespace au travers d'échange entre États. On parle de « mesures de renforcement de la confiance ».

Les mesures de transparence	Elles consistent à partager publiquement toute information apte à apaiser les autres États face à la perspective d'un différend : partage de points de contacts techniques et diplomatiques afin de faciliter les échanges ; partage de la stratégie nationale de cybersécurité… mais aussi doctrine cyber offensive et des conditions d'emploi de ces capacités, etc.
Les mesures de coopération	Elles consistent en l'ensemble des mécanismes de coopération, notamment techniques entre équipes de réponse à incidents (CSIRTs) permettant au quotidien d'œuvrer collectivement à identifier les vulnérabilités et rendre les systèmes d'information plus sûr, mais aussi au niveau diplomatique ou politique, permettant de résoudre de manière pacifique d'éventuels différends.
Les mesures de stabilité	Ces dernières consistent en l'établissement de mécanismes de signalement et de dialogue en vue de permettre une désescalade entre Etats en cas de différend et de perspective de conflit, le plus souvent au niveau politique. C'est, par exemple, le cas entre les Etats-Unis et la Russie qui ont mis en place une ligne de signalement d'urgence en cas d'attaque.

Fixer les règles pour un cyberespace stable et sécurisé

Au-delà du renforcement de la confiance, le cyberespace doit être protégé par le droit international afin d'encadrer les actions des États, éviter la survenue de conflits entre eux ou encadrer ces derniers. A cette fin, deux axes de travail guident depuis plusieurs années des travaux entre diplomates principalement à l'ONU.

Les normes de comportement responsables des États dans le cyberespace	Non contraignantes, ces normes de comportement, décrites dans plusieurs rapports de l'ONU (notamment le rapport de 2015), proposent les comportements que les États devraient adopter pour prévenir les incidents cyber et y répondre, en priorité par la coopération.
L'application du droit international au cyberespace	Les discussions à l'ONU portent également sur les modalités d'application du droit international au cyberespace. Par exemple, quelles sont les conditions d'exercice du droit à la légitime défense des États face à des cyberattaques comme prévu par l'article 51 de la Charte des Nations Unies ?

L'appel de Paris

La sécurité et la stabilité du cyberespace n'étant pas que l'affaire des États mais aussi des acteurs non étatiques et des entreprises, l'appel de Paris lancé par la France en 2018 a réuni + de 500 entités du monde entier pour appeler au renforcement de la confiance et de la sécurité dans le cyberespace.

Une brève histoire de la cybersécurité

La cybersécurité : un domaine aux racines très anciennes...

Si l'on pourrait croire que la cybersécurité est un domaine très lié aux « nouvelles technologies » et donc relativement récent, elle trouve en fait ses racines dans un sujet vieux de plusieurs siècles : la cryptographie (voir les fiches consacrées à la cryptographie). Au fur et à mesure de la création des États, les dirigeants ont, en effet, ressenti le besoin de protéger leurs secrets – politiques, stratégiques et diplomatiques– des puissances étrangères. Jules César est à cet égard un exemple célèbre et très ancien de chef d'État qui a recouru à la cryptographie pour protéger ses correspondances.

Entre les années 1200 et 1650, la construction de l'État français tel que nous le connaissons est passée par des étapes importantes, qui ont contribué à structurer son organisation et ses missions les plus essentielles : création des Archives nationales, du Trésor, d'une monnaie unique dans tout le royaume, d'un impôt (la taille) permettant de lever une armée permanente ou encore des postes. A partir de 1600 environ et jusqu'à la Révolution française, une fonction de « cryptographe du Roy » sera ainsi tenue à plein temps. L'un d'entre eux, Antoine Rossignol sera, par exemple, remarqué par le cardinal de Richelieu. Il servira pendant plus de 50 ans les rois Louis XIII puis Louis XIV et ira jusqu'à transmettre sa fonction à son fils et son petit-fils, avec pour mission de chiffrer et déchiffrer les correspondances du Roi et lui transmettre directement les résultats des messages interceptés.

La sécurité des communications, au cœur des grands conflits mondiaux

La protection des communications des autorités politiques et militaires a pris une importance critique lors des grands conflits mondiaux. Pendant la première guerre mondiale, la France dispose ainsi d'une équipe chargée de travailler sur les messages allemands interceptés pour en « casser » le chiffrement. En juin 1918, dans une séquence épique et héroïque, Georges Painvain, jeune et brillant officier affecté à cette unité, réussira à percer les codes allemands pour décrypter le « Radiogramme de la Victoire ». Transmise aux hautes autorités politiques et militaires, cette information permettra aux Français d'anticiper les mouvements adverses et de mener une contre-offensive décisive pour barrer la route aux troupes ennemies, jouant un rôle capital dans la tournure du conflit.

Durant la seconde guerre mondiale, le « Chiffre » joue de nouveau un rôle central. Le film « Imitation Game » a contribué à faire connaître l'action de personnages illustres tels qu'Alan Turing – considéré comme l'un des fondateurs de l'informatique moderne – dans la cryptanalyse de la machine de chiffrement Enigma, utilisée par les Allemands pour protéger le secret de leurs échanges. Au-delà du rôle des britanniques, un travail fondamental a été mené par les français, derrière le général Gustave Bertrand, en collaboration avec de brillants mathématiciens polonais tels que Marian Rejewski[1].

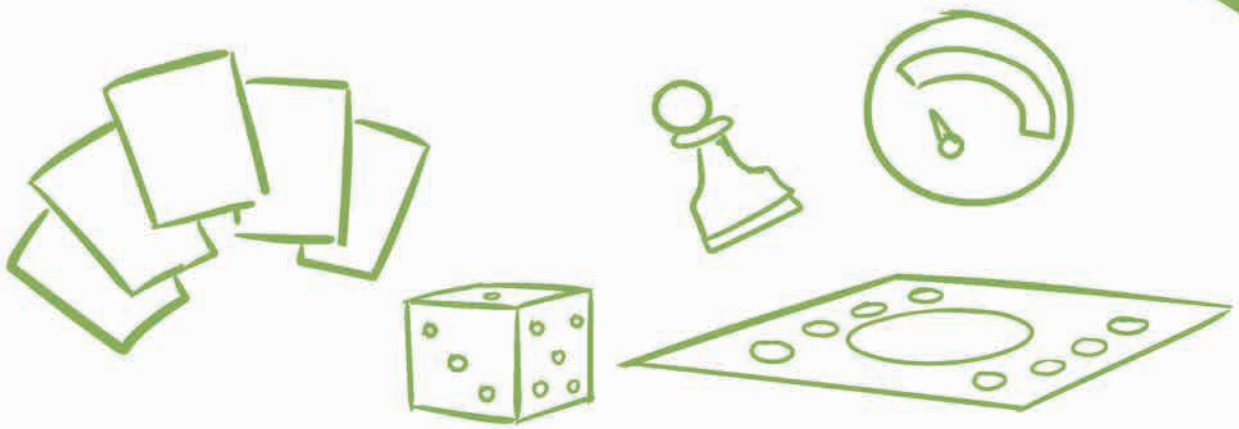
1. L'excellent ouvrage « Enigma, ou comment les Alliés ont réussi à casser le code nazi », de Dermot Turing, neveu d'Alan Turing, est une référence complémentaire précieuse sur cet épisode.

MATÉRIEL DE PROTOTYPAGE

Ce que ce matériel vous permet de faire et comment

Cette liste d'outils et d'objets à imprimer vous est proposée pour commencer à prototyper des jeux. Vous pouvez aussi faire appel à tous les objets à votre disposition pour créer vos prototypes, dans une logique de réusage et de création de jeux low tech.

Matériel de prototypage inclus dans le kit physique



Les éléments physiques de ce kit sont là pour vous inspirer des mécaniques de jeu à testeret faciliter le passage au prototypage.

Voici ce qui est inclus dans le kit : 1 dé, des cartes, 5 pions de plusieurs couleurs, des compteurs de points, un plateau à personnaliser, du matériel de prototypage effaçables est également inclus ainsi qu'une chiffonnette et les impressions des fiches du kit.

Pour rappel, voici trois directions que vous pouvez prendre pour commencer à prototyper avec ce kit :

1. Créer un serious game
2. Créer une session de jeu
3. Créer un hackathon

Voici quelques exemples complémentaires pour vous inspirer : jeux de cartes, challenges sur table, compétition, jeux de storytelling ou d'improvisation, enigmes, escape games, session de game design, bandes dessinées, jeux de storytelling ou encore concours de création de jeux !

->Vous pouvez rajouter ce que vous avez à portée de main et qui vous inspire, comme du matériel issu d'autres jeux que vous avez à la maison.

Voici comment vous pouvez commencer à prototyper rapidement avec ce matériel :

Les **cartes "objectifs pédagogiques"** sont un très bon point de départ pour utiliser le kit. Sélectionnez-en 1 ou 2. En plus des objectifs de jeu que vous pourrez imaginer, cela sera votre curseur pour évaluer les retours pédagogiques. Dès que vous les avez sélectionnés, commencez par travailler votre sujet et commencez à utiliser certains éléments parmi le matériel de prototypage. Des cartes peuvent devenir des personnages, un dé des options ou encore un plateau de jeu un parcours représentant un processus !

Les **fiches sur la cybersécurité** sont remplies d'informations très utiles pour concevoir votre jeu. Ces informations vous aideront à enrichir vos jeux et à utiliser vos supports. Par exemple, la fiche cryptographie vous donne un très bon point de départ pour imaginer des énigmes et pratiquer cette discipline pour décoder un message.

Bien sûr, vous pouvez compléter avec vos connaissances et vos recherches.

Les Fiche Organisations vous donneront plus d'informations sur l'utilisation de ce kit avec des groupes.

Liste d'outils pour créer des jeux

Un certain nombre d'outils sont librement accessibles en ligne afin de créer des prototypes numériques ou bien encore des prototypes physiques de jeux.

Autre outils pour le prototypages

Vous pouvez parfaitement prototyper votre propre matériel de jeu avec des impressions de supports trouvés en ligne.

Pour trouver les ressources adaptées à votre projet, nous vous conseillons d'aller faire un tour sur Open Serious Games. De nombreuses ressources comme leur blog vous permettront d'identifier le bon support pour votre jeu, de vous inspirer des créations d'autres personnes et de vous renseigner sur les mécaniques de jeu à utiliser.

Outils pour le prototypage numérique

Si vous voulez prototyper votre jeu sur un support digital, vous pouvez choisir un support comme un site internet, un outil collaboratif ou l'utilisation de données en ligne. Pour ce faire, vous pouvez privilégier les outils en no code pour aller au plus simple.

Si vous voulez partir sur la création d'un jeu vidéo, il y a plusieurs logiciels qui pourront vous être utiles en fonction de votre niveau. Vous pouvez consulter les articles de blog du site Clubic pour vous orienter.

A vous de jouer !

Version bêta - juin 2021