التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

LES JEUX VIDÉO, UN MOYEN DE RECRUTEMENT POUR LES TERRORISTES

Préparé par: Département des études et des recherches

Mars 2023

3 Questions de terrorisme

Questions de Terrorisme

Numéro mensuel - Coalition Islamique Militaire Contre le terrorisme

---

Superviseur général

Major-Général Mohammed bin Saïd Al-Mughaidi

Secrétaire Général désigné de la Coalition Islamique Militaire Contre le Terrorisme

---

Rédacteur en chef

Ashour Ibrahim Aljuhani

Directeur du Département des Études et des Recherches

LES JEUX VIDÉO, UN MOYEN DE RECRUTEMENT POUR LES TERRORISTES

PRÉPARÉ PAR: DÉPARTEMENT DES ÉTUDES ET DES RECHERCHES

Au cours du siècle écoulé, le monde a vécu une révolution impétueuse en matière d'information et de technologie. Laquelle révolution a promptement contribué au développement tangible des formes variées des E-services, assurés par tous les secteurs, aussi bien gouvernementaux que privés. Cette révolution a également bouleversé les modes de vie des différentes communautés, et a touché à leurs habitudes, pratiques, comportements et valeurs. Du coup, nos sociétés ont été amenées à abandonner nombres de leurs us et coutumes séculaires, d'où l'intervention, quant à l'éducation sociale fournie aux nouvelles générations, de multiples facteurs, dont en premier lieu la E-culture qui joue un rôle considérable dans la formation des valeurs et des tendances culturelles et civilisationnelles.

Comme le monde est devenu un village planétaire, à force de l'Internet à portée de tous, il s'est avéré impératif pour chaque État d'œuvrer en vue de protéger ses sujets, ses institutions, ses ressources et sa civilisation contre l'impact des accès sans borne. Si les utilisateurs du réseau Internet sont conscients des bienfaits de la technologie de l'information, ils doivent être en même temps conscients des risques inhérents de la technologie que peuvent subir les membres de la société. De là, la société et les institutions gouvernementales sont préconisées de juguler ces risques.

En fait, les utilisateurs des jeux vidéo, fort répandus parmi les enfants et les jeunes, acquièrent des valeurs et des inclinations intellectuelles et comportementales variées, si bien que ces jeux rivalisent du rôle de la famille dans la formation de la personnalité des joueurs, d'où l'apparition d'une éducation sociale, incompatible avec les us et coutumes adoptés dans la société [1].

Cependant, il ne faut pas nier que ces jeux constituent à présent un fait accompli et une source importante d'éducation sociale, compte tenu de l'influence directe qu'ils exercent sur le comportement des individus et des communautés. Il est donc nécessaire de contrôler le temps que les enfants et les jeunes passent devant ces jeux [2].

À la lumière de ces effets des jeux vidéo, la mission des groupes terroristes dans le recrutement des enfants et des jeunes est devenue de plus en plus aisée. Puisque les enfants et les jeunes ne possèdent encore pas la culture nécessaire pour distinguer les pensées saines des idées extrémistes et takfiris (d'excommunication), il est facile pour les groupes terroristes de mettre dans leur tête des idées erronées, des notions apocryphes et des croyances défectueuses, qui aident à les recruter

par le biais des jeux vidéo auxquels ils s'adonnent. En fait, les jeux vidéo qui contiennent des guerres, des explosions, des meurtres, du sabotage, de la violence et du terrorisme contribuent à la programmation mentale des enfants et des jeunes, de sorte qu'ils se familiarisent à ces scènes et s'enthousiasment à les appliquer dans la vie réelle.

De là, nombre d'États ont eu recours à des mesures préventives face au cyberterrorisme. Or, leurs efforts ont besoin d'être affermis par davantage de procédures pour faire face à ce danger, compte tenu de ses ressources, dimensions et objectifs variés. Nous pouvons même dire que le cyberterrorisme est la menace de l'avenir, qui a des formes, des tactiques et des domaines multiples, ce qui requiert des stratégies de lutte créatives et de pointe.

Le cyberterrorisme :

Le terme du « cyberterrorisme » est apparu dans les années 80 du siècle passé pour désigner les attaques électroniques contre les économies et les gouvernements étatiques. Le sens du terme a pris de l'envergure au début des années 90 du même siècle, avec l'usage accru de la connexion Internet, surtout dans les relations internationales ; un usage qui s'est affirmé clairement dans les événements du Printemps arabe.

Définition du « cyberterrorisme » :

Il existe plutôt plusieurs définitions au terme du « cyberterrorisme », qui désignent toutes une culture négative et une forme de terrorisme, issue du développement technologique et de la révolution de l'information, et basée sur l'exploit du réseau Internet et des dispositifs techniques pour commettre des crimes, dont la destruction, le sabotage et le pillage.

Ainsi pouvons-nous définir le cyberterrorisme en tant que l'agression, la propagation de l'effroi ou la menace matérielle et morale, qui sont commises ou qui ciblent des États, des groupes ou des individus, à l'aide de dispositifs électroniques via le cyberespace, d'une manière qui déroge à l'usage pacifique auquel ces dispositifs sont destinés à l'origine [3].

Nous pouvons également le définir comme étant l'emploi des technologies numériques dans le but d'intimider ou dompter autrui, ou d'attaquer les systèmes d'information pour des motifs politiques, économiques, sociaux, raciaux, doctrinaux ou intellectuels.

Selon une troisième définition, le cyberterrorisme est l'agression, l'intimidation ou la menace matérielle ou morale, commises par des États, des groupes ou des individus, à l'aide des moyens électroniques, pour assaillir sans droit, et par tous les moyens de la propagation de la corruption sur terre, la religion, l'âme, l'honneur, l'esprit ou les biens d'une personne [4].

Les formes du cyberterrorisme :

Le cyberterrorisme peut prendre les formes suivantes:[5]

- L'usage, par les terroristes, des plateformes électroniques pour communiquer avec leurs complices et leurs bailleurs de fonds, effectuer une coordination avec eux et leur donner des ordres pour l'exécution des opérations terroristes.
- La création de sites web, consacrés aux campagnes médiatiques menées contre les pays cibles. Les administrateurs de ces sites web publient les photos des otages et des prisonniers ou de leur exécution, ou répandent les rumeurs susceptibles d'ébranler la sécurité et l'économie de l'État ou du groupe cibles, ou lancent les appels pour faire éclater les manifestations et les actes de vandalisme dans les pays cibles.
- Le piratage des ordinateurs pour les manipuler ou les saper. Selon les études psychologiques sur les traits personnels des pirates informatiques, ceux-ci souffrent souvent de maladies psychiques qui les poussent à s'insurger contre la société ou ses institutions, d'où leur inclination vers la manipulation et la destruction.
- La mainmise sur les biens ou les dossiers personnels d'autrui, du fait que celui qui pirate l'ordinateur personnel d'un individu s'empare ainsi de ses propriétés. Le recours aux dispositifs de la technologie moderne pour dépister des informations personnelles qui appartiennent à des individus ou à des institutions, puis les extorquer et les menacer de les publier sur le réseau Internet, s'ils ne se plient pas aux demandes des pirates.
- L'endoctrinement électronique. C'est le fait de rassembler ceux qui corroborent ou qui compatissent avec leurs principes, méthodes et procédés, dans une tentative de mobiliser et de recruter de nouveaux terroristes via les réseaux sociaux et les salles de discussions (chat rooms) des jeux vidéo.

Les jeux vidéo :

Les jeux vidéo ont fait leur apparition avec les prémices de l'industrie informatique. Ils ont alors compté sur les potentiels disponibles pour simuler la réalité et inventer des éléments virtuels, ouvrant ainsi aux utilisateurs de nombreux domaines interactifs d'apprentissage et de divertissement. Cela a amené les compagnies spécialisées à développer les appareils et les logiciels de ces jeux, afin de promouvoir la conscience socio-culturelle.

Au cours des quelques dernières années, les points de vente des jeux vidéo et les salles de jeux se sont parsemés partout. Les enfants et les jeunes ont éprouvé une demande accrue pour se procurer de ces jeux vidéo, lesquels se sont répandus dans les maisons, les clubs et les centres de jeux, et stimulent en principe la vigilance, la concentration et la réflexion. [6]

Le développement des appareils électroniques et

l'augmentation de leur nombre ont été accompagnés d'une évolution des jeux vidéo. Ils sont passés des jeux tactiques de vitesse et de suspense aux luttes entre les animaux féroces pour finir par représenter des guerres virtuelles entre les pays, les bandits ou les milices. Désormais, ils contiennent des stratégies militaires et des engins de guerre, légers et lourds, et leurs histoires sont fondées sur la destruction, les meurtres, le saccage et le pillage. Avec le développement technologique accéléré, les jeux vidéo sont devenus en vogue et attirent les joueurs de toutes les catégories d'âge.

Or, ces jeux sont devenus hors de contrôle : ils permettent aux enfants et aux jeunes de contribuer à leurs fabrication ou à leur programmation, et leur inculquent des valeurs sociales, peut-être au détriment de celles de nos communautés. Par conséquent, la loyauté et l'appartenance de l'enfant à sa société fléchissent. Parfois même, ces jeux présentent aux enfants des contenus sociaux tordus qui peuvent faire d'eux de véritables ennemis à leur patrie. [7]

Types de jeux vidéo :

Les jeux vidéo se divisent aux types suivants :

- Des jeux fondés sur une histoire ou un personnage de dessin animé, et ce type de jeux est très utile.
- Des jeux de réflexion qui stimulent l'imagination, l'agilité d'esprit, la bonne mémoire et l'activité mentale.
- Des jeux de stratégie militaire et de plans de guerre, qui requièrent une maturité mentale.
- Des jeux qui orbitent autour de la lutte pour la survie.

Quoique violents, ce type de jeux entraînent la passivité intellectuelle et mentale, car ils sont animés par les meurtres, la destruction, le sabotage et l'extase. [8]

La propagation des jeux vidéo constitue un phénomène dangereux, surtout à l'absence d'une législation qui interdit leur vente aux enfants. De plus, certains téléchargent ces jeux sur Internet via les sites étrangers ou de manière illégale sur les sites arabes, puis les modifient de sorte qu'il contienne par exemple un plan stratégique, mis par un groupe de joueurs pour voler une banque ou un magasin. Selon ce plan, les joueurs sont amenés à porter des masques ou à déguiser leurs personnalités. Or, ce genre de jeux incitent les joueurs à commettre les tueries, à saccager les biens d'autrui, et à faire fi des lois et des systèmes de sécurité.

En fait, l'aspect négatif des jeux vidéo réside en principe dans leurs thèmes venimeux, dont la violence, le sexe, ou l'indifférence vis-à-vis d'autrui. Peu de ces jeux sont conçus pour la distraction anodine ou pour des objectifs éducationnels précis, alors que la majorité d'entre eux visent à standardiser les besoins de divertissement chez les jeunes, et concourent pour faire des vices virtuels, dont le meurtre, la violence, l'escroquerie ou le mensonge, des produits récréatifs, destinés à des groupes d'âge, encore incapables de résister à leurs menaces à cause de leur faible conscience, étant dans les premières phases de l'acquisition et de la formation. [9]

Le rapport entre la violence dans les jeux vidéo et le cyberterrorisme :

La plupart des jeux vidéo contiennent des stéréotypes de personnages au comportement violent, que les enfants et les jeunes se complaisent d'imiter. Cependant, leur attitude ne se heurte point à la moindre critique ou condamnation, susceptibles de faire valoir l'opinion sociale qui considère la violence comme un comportement réprouvé auquel il faut résister.

Cela coïncide d'une part avec l'absence notoire du contrôle de la famille, quant aux jeux vidéo, et d'autre part avec l'apparition de nouvelles couches sociales, distinguées les unes des autres par le degré de leur familiarité avec la technologie de l'information et de leur conscience vis-à-vis de ses risques éventuels. Il faut prendre en compte que le niveau de la conscience culturelle chez maintes catégories de la société les rend insensibles aux dangers des jeux vidéo en général. [10]

Donc, les jeux vidéo, commercialisés par les organisations terroristes correspondent à un processus de recrutement organisé des enfants et des jeunes. Il est à remarquer que la majorité de ces jeux contiennent une grande variété d'armes, fusils, pistolets, couteaux, épées, utilisées pour produire la ruine, accaparer les biens des autres et semer la terreur. Par conséquent, ces jeux altèrent la nature innée saine des enfants et des jeunes, les écartent entièrement de leur environnement pour les placer dans un autre, animé par la violence, les meurtres, la destruction et la misanthropie [11].

Cet environnement virtuel leur apprend le fanatisme religieux et sectaire, et le non-respect des règles de sécurité, et affaiblissent chez eux le sens de responsabilité sociale, soit des valeurs hostiles à la bonne citoyenneté.

Les méfaits des jeux vidéo ne se limitent pas à la violence qui anime leur univers virtuel. Ils désorientent les jeunes pour faciliter leur adhésion aux organisations terroristes. Les membres de ces organisations s'adressent vocalement aux joueurs via Internet, pour les déconcerter et les fourvoyer. Encore plus, ils communiquent parfois entre eux pour mettre leurs

opérations terroristes à exécution : ils se mêlent au jeu, simulent une bataille, mettent les plans stratégiques et échangent entre eux dans ce monde virtuel, loin de la surveillance directe des appareils de sécurité, d'autant plus que les serveurs auxquels ces jeux sont connectés sont éparpillés partout dans le monde. Les organisations terroristes essayent de prendre contact avec les joueurs, à l'aide des discussions vocales ou textuelles, et essayent de les dévoyer. Il est plausible que les enfants et les adolescents, influencés par ces suggestions et ayant la frénésie de vivre dans la réalité les aventures violentes des jeux vidéo, deviennent la proie de ces tentatives.

Le rapport entre le comportement violent dans les jeux vidéo et le cyberterrorisme :

Les enfants et les jeunes qui s'adonnent aux jeux vidéo animés par la violence peuvent avoir des idées et des comportements agressifs. Cela rend ces jeux plus pernicieux que les films de violence, diffusés sur les écrans de la télévision ou du cinéma, du fait de la nature interactive de ces premiers. En s'adonnant à ces jeux, l'enfant se fait passer par son personnage batailleurs, ce qui lui insinue l'idée que le meurtre est une chose admissible et amusante.

Le danger des jeux vidéo réside dans la consolidation constante du comportement meurtrier ou destructif, entre autres pratiques agressives. Dans ces jeux, le gagnant est celui qui enregistre le taux le plus élevé de destruction et d'effusion de sang, et ce résultat est abordable lorsque le joueur se voue entièrement aux temps et lieu virtuels du jeu. Du coup, il recourt aux solutions violentes face aux autres joueurs, pour traverser les obstacles qui peuvent l'empêcher d'enregistrer le nombre de points requis pour atteindre les niveaux finaux du jeu. Il obtient des prix et des incentives en échange des meurtres et des ruines qu'il produit tout au long de la durée du jeu. Là, l'enfant se trouve dans un cercle vicieux de violence et d'agression, puisque la récompense qui bénit de ce comportement est abondante. En d'autres termes, le joueur qui maîtrise le plus les actes de violence et d'agression est le gagnant. [12]

Donc, le recours à la violence est récompensé, selon la conception de ces jeux et en fonction des options qu'ils offrent, ce qui ouvre la voie devant les joueurs, et notamment ceux parmi eux qui sont de jeune âge ou qui ont tendance aux aventures et à la violence, à pratiquer des solutions violentes et un comportement agressif lors des conflits ou des compétitions. De là, ces jeux se prévalent des idées violentes, mettant la vie des jeunes en danger, puisque les jeunes, comme les enfants, jouent et apprennent en même temps. Cette hypothèse se manifeste clairement dans les intrigues menées par les joueurs ou dans les plans agressifs qu'ils mettent en œuvre.

Quant aux groupes terroristes, ils peuvent profiter de ces jeux pour enrôler de nouveaux membres, surtout parmi les enfants et les jeunes. Ainsi, les jeux vidéo qui se glorifient de la mort en martyr sont-ils susceptibles d'attirer l'attention des futurs kamikazes. D'ailleurs, ces groupes peuvent profiter des jeux vidéo pour des objectifs didactiques indirects, en encourageant les enfants et les jeunes à cambrioler les maisons, les biens, les voitures ou les banques, à faire sauter les bâtiments et à commettre des homicides. [13]

Peu-à-peu, les jeux vidéo font de la violence une attitude et un comportement ordinaires, adoptés par leurs fans comme étant la seule méthode à utiliser face aux discordes qui peuvent survenir dans la vie sociale réelle. De plus, ils révèlent aux enfants et aux jeunes les moyens de commettre un crime, ainsi que les arts et les astuces criminels ; ils développement chez eux les compétences mentales de la criminalité, les disposent à exercer les actes terroristes et les poussent même à faire partie des organisations terroristes. [14]

Les jeux vidéo, un moyen de recrutement pour les groupes terroristes :

Les terroristes profitent, dans une large mesure, des jeux vidéo connectés au réseau Internet pour divulguer la pensée extrémiste, les croyances apocryphes et les idées erronées, qui leur facilitent la mission du recrutement de nouveaux membres dans les organisations terroristes ou de nouveaux kamikazes. Pour ce faire, ils simulent des clips qui motivent ce recrutement et les intègrent dans le jeu vidéo. Ce procédé a abouti et les groupes terroristes sont parvenus à se faire une propagande de grande envergure de manière rapide et efficace. En conséquence, au cours des quelques dernières années, ce phénomène est devenu une menace mondiale, après que les terroristes ont pu, par ce procédé, atteindre un plus grand nombre de partisans, d'où une montée tangible dans le nombre de terroristes enrôlés et, par conséquent, dans le nombre des attaques terroristes partout dans le monde, surtout celles mises en œuvre par les loups solitaires et les cellules dormantes. [15]

De là, nombre de groupes terroristes ont retranché une bonne partie de leurs ressources et de leurs potentiels

au monde de l'Internet, et notamment aux jeux vidéo, ce qui rend de plus en plus difficile aux appareils de sécurité de poursuivre les activités terroristes ou de cerner leur propagation.

C'est pourquoi les appareils de sécurité, les spécialistes et les experts sécuritaires sont prônés de consulter au fur et à mesure les législations relatives à la cybersécurité, afin de prendre en considération les effets néfastes des jeux vidéo violents sur les joueurs, lors de l'élaboration de la politique générale – de pair avec les procédures de la lutte antiterroriste – qui facilitent le dépistage et l'arrestation des terroristes à la l'aide de la technologie moderne.

Le réseau Internet a donné davantage d'occasions aux terroristes pour œuvrer en catimini, et à l'abri de la surveillance sécuritaire, en vue de cibler certaines catégories par leurs messages et idées venimeuses, de former leurs partisans, de collecter les fonds et de mettre les plans de leurs attaques terroristes [14]. Ils comptent surtout sur l'interaction, qui a élargi le périmètre de leurs contacts via Internet, puisque le réseau Internet vainc les frontières géographiques et les obstacles sécuritaires. Ainsi, ils communiquent entre eux à partir de n'importe quel endroit dans le monde, sans surveillance ni bornes. Quoique le développement de la TI ait stimulé une croissance socio-économique, nombre de médias et de réseaux sociaux, dont Facebook, tirent profit du contenu qui provoque la sympathie des lecteurs, comme les photos des actes de violence ou les clips de meurtre. Les informations sensibles animent chez eux des sentiments contradictoires, d'où les discussions et l'interaction intense sur les réseaux sociaux, et l'augmentation des nombres de vues et de commentaires, ce qui rend le système social plus populaire et plus solide. Souvent, ces réseaux sociaux répètent la publication du contenu ou négligent sa suppression pour réaliser des gains économiques. Ils véhiculent ainsi les prévisions, au lieu de bloquer complètement et immédiatement le contenu violent et importun [16]. De là, les États sont préconisés de résoudre cette dilemme, tout d'abord par les amendements législatives, avant d'entreprendre une lutte contre le terrorisme et l'extrémisme cybernétiques.

Par ailleurs, la pandémie du Covid-19 a poussé beaucoup de gens à passer davantage de temps sur l'Internet, ce qui les a rendus plus exposés au contenu extrémiste, à l'extrémisme et à l'implication dans la violence [17]. Ces circonstances ont occasionné aux terroristes un grand nombre de faibles cibles, vulnérables aux méthodes de l'extrémisme qu'ils utilisent. Par exemple, comme les gens ont été récemment à la recherche des sites de divertissement et de jeux vidéo, afin d'appartenir à un univers virtuel où ils peuvent interagir avec des personnes aux quatre coins du monde, la popularité des jeux vidéo et leur capacité d'atteindre une audience variée sont montées en flèche. À cette époque, maintes organisations terroristes ont œuvré en vue d'attirer davantage de combattants et d'alliés, et de les préparer pour commettre des actes de violence, sans avoir des rapports physiques avec les activités terroristes [18].

Les plateformes de ces organisations terroristes diffusent via Internet des jeux vidéo, qui permettent au joueur de se faire une émission audiovisuelle directe, pour partager son expérience dans ces jeux avec les autres joueurs. Cependant, certains ont utiliser les salles de discussions pour faire la propagande de leurs points de vue politiques violents à propos des questions controversées.

D'autre part, une enquête est menée à présent au sujet des jeux vidéo où une personne tire sur une autre. Cette enquête vise à déduire leur effet probable qui consiste à rendre les joueurs insensibles à la violence, ou à faire la propagande de la violence. Selon une étude, effectuée par l'Université de la Californie du Nord à Chapel Hill, aux États-Unis, les groupes terroristes ont modifié leurs stratégies de recrutement, de sorte à utiliser les jeux vidéo violent pour que les éventuelles personnes enrôlées trouvent attractive l'adhésion à ces groupes. Les chercheurs ont découvert que les clips de la propagande et du recrutement de Daech calquent les jeux vidéo, dont en premier lieu la série « Call of Duty ». De même, les éditions de « First Person Shooter » (Jeu de tir à la première personne) sont jouées par des millions de personnes jusqu'à l'âge de 35 ans ; 90% des joueurs sont des hommes. Ce taux est un objectif démographique primordial des organisations terroristes.

En outre, les clips publiés par Daech simulent les scènes et les traits distinctifs de ces jeux de manière détaillée, de sorte que les joueurs ordinaires puissent les reconnaître. Ces jeux contiennent des scènes qui incitent au terrorisme, comme la manière dont le tireur porte l'arme, ou les images des armes des plus légères aux plus lourdes, ou les clips des drones, ou le moyen d'utiliser les cartes topographiques ou les adresses [19]. Selon les chercheurs, les jeux vidéo n'ont pas un rapport direct avec l'extrémisme des joueurs. Cependant, les groupes terroristes, dont Daech, ont conçu leurs

stratégie de recrutement de manière homologue à celle qui se trouve dans les jeux, dont « Call of Duty » ou « First Person Shooter », et de sorte à montrer, dans les clips concernant le recrutement, les armes à feu en vue subjective [20]. Il faut noter que les créateurs des jeux vidéo ne commercialisent pas la violence, mais cherchent les gains matériels. Et pourtant, les organisations terroristes, comme Daech, conscientes de la popularité des jeux de tir en vue subjective, ont décidé que, par le recours à la technologie des jeux FPS, elles peuvent arriver à une audience plus dense, parmi laquelle il y aura de nouveaux membres à enrôler.

Or, Daech en particulier est connu par son attitude qui encourage la violence contre les petits enfants par des moyens de divertissement ayant trait à la technologie. Il s'agit surtout de l'application didactique « Huroof », qui demande aux enfants de lier chaque lettre arabe à l'image des grenades, des armes, des chars et des autres symboles militaires correspondants [21]. Il est vrai que les enfants sont faibles, mais leur acquisition scientifique est rapide. Cette méthode de divertissement daechiste qui cible cette tranche démographie peut fort probablement entraîner la création d'une nouvelle génération de combattants déterminés, fidèles à la cause de Daech, sans égard aux valeurs morales ni à la ruine issue de la violence. Cette hypothèse doit trouver un remède au niveau international : il faut prendre les mesures nécessaires pour garantir une éducation saine à ces enfants, qui substitue aux tactiques des groupes terroristes.

Daech n'est pas le seul groupe terroriste qui se focalise sur les jeux vidéo et sur les autres plateformes sur Internet. Les autres organisations terroristes, et les moins évoluées, ont été inspirées par les stratégies de recrutement de Daech, et ont commencé à les adopter. La même équipe de recherche de l'Université de la Californie du Nord à Chapel Hill a analysé les éléments qui composent les technologies de recrutement, puisées du jeu FPS, et les a comparés à leurs produits. L'équipe a étudié la stratégie des jeux vidéo susmentionnés à la lumière de 50 points évaluatifs, qui s'étendent sur les valeurs de la production artistique, l'histoire, la caméra, la rédaction, etc. En utilisant cette échelle de notation, les chercheurs ont déduit que la production de la vidéo exemplaire de Daech copie de manière professionnelle celle des compagnies productrices des jeux [20]. En fait, le recours à ces technologies dans le recrutement prouve, sans l'ombre d'un doute, que les organisations terroristes sont devenues de plus en plus sophistiquées. Elles adaptent leurs stratégies d'attractivité engagée aux intérêts de la tranche démographique ciblée, et élaborent des campagnes de recrutement séduisantes. Elles sont prêtes à apprendre, à pratiquer et à utiliser les différentes compétences, que les personnes ordinaires ne considèrent pas comme une menace.

Au fur et à mesure que ces tactiques revêtent de popularité, les organisations terroristes rivalisent entre elles pour optimiser leurs stratégies d'enrôlement et arriver au plus grand nombre de recrues potentiels. Les efforts s'amplifient pour détecter ces derniers et pour attirer d'autres affiliés, ce qui prouve que la menace du cyberterrorisme continuera ouvertement à se développer et à s'adapter avec les préférences populaires, repérées à notre époque moderne.

Si l'on juge négatif le recours, par les organisations terroristes, aux technologies de pointe dans le recrutement, l'extension accrue de ces technologies via les jeux vidéo peut conduire les appareils sécuritaires à repérer les organisations terroristes. En fait, l'examen minutieux des clips de propagande peut contribuer à poursuivre le déploiement des méthodes de production évoluées, et à ressortir des empreintes esthétiques, capables de déterminer les groupes et les organisations qui produisent ces matières [23]. L'analyse de ces clips, produits par les organisations extrémistes, peut permettre aux autorités chargées d'appliquer la loi, de concert avec les responsables gouvernementaux, de condamner ces pratiques en public, de les prévenir aux niveaux local et international, et d'accroître ainsi la vigilance face aux inconnus rencontrés sur les réseaux sociaux. Aussi, la stigmatisation des technologies évoluées des terroristes, à l'aide des bulletins d'information, des sources imprimées et des discours, peut aider les personnes ordinaires à comprendre les stratégies dont se servent de nos jours les terroristes et, par conséquent, à découvrir l'activité terroriste, une fois rencontrée, et à la dénoncer. De leur côté, les agences, organisations et compagnies doivent augmenter le financement accordé aux département et aux employés de la cybersécurité, afin d'optimiser les mesures qu'ils entreprennent pour sonder l'Internet à la recherche d'une langue ou d'une photo ayant trait à l'extrémisme. Elles doivent également nouer des partenariats avec les grandes compagnies de technologie pour garantir leur coopération dans ce processus, de sorte que les unes et les autres s'engagent à protéger les utilisateurs des démarches des terroristes.

Un tournant est survenu dans la lutte de l'extrémisme

via Internet, lorsqu'un nombre d'applications de chat collectif, appartenant à des groupes extrémistes violents, ont été bloquées et supprimées des serveurs. C'est le cas par exemple de « Discord », qui est une application de chat collectif, conçue en principe en faveur des joueurs. « Discord » a supprimé les groupes qui ont été créés pour parler de la violence et des idéologies extrémistes [24]. Cette mesure est importante, puisqu'elle prouve que les plateformes de réseaux sociaux ont le pouvoir de contrôler tout ce qui se passe à l'intérieur, bien que la détection du contenu violent soit compliquée, mais faisable. Ainsi, le blocage des groupes qui prêchent la violence peut être un avertissement préventif à tous ceux qui pensent créer leur propre groupe extrémiste.

Le groupe de lutte antiterroriste œuvre en vue de surveiller et d'analyser le contenu extrémiste et terroriste, publié sur toutes les plateformes sur Internet, puis émet des rapports susceptibles d'en dépister les auteurs, et de définir les nouvelles technologies à consulter. Il tient toujours l'équipe de lutte antiterroriste au courant des dernières lois relatives à la confidentialité des jeux vidéo violents, et retrace les liens nécessaires à l'analyse, pour éviter que les organisations extrémistes profitent des éventuelles lacunes ou contreviennent à la politique publique. Quant aux brigades criminelles, elles donnent la priorité au renseignement qui révèle les opérations de l'extrémisme terroriste, et qui est collecté des plateformes médiatiques réputées, comme « Twitch », consultée chaque mois par quelque 140 millions visiteurs [25].

La cybersécurité :

La cybersécurité ressemble aux forces de sécurité régulières, chargées de protéger les propriétés et les âmes contre les activités criminelles ou terroristes. De même, la cybersécurité protège les systèmes informatiques, les applications des utilisateurs finaux, les utilisateurs de ces systèmes informatiques, ainsi que les informations stockées.

Autrement dit, la cybersécurité empêche les cybercriminels, les pirates et autres d'accéder aux systèmes informatiques ou aux applications de la TI pour les endommager, les mettre en panne ou les modifier.

L'importance de la cybersécurité :

De nos jours, la digitalisation a intégré la communauté humaine, et a touché tous les aspects de leur vie, par le biais des réseaux Internet, des ordinateurs, des appareils électroniques et des logiciels. Elle est devenue une partie intégrante à l'infrastructure vitale, si bien qu'elle intervient dans la protection sanitaire, dans les institutions financières, dans les gouvernements, dans l'industrie, dans les PC et dans les appareils intelligents, comme partie principale de leurs opérations, et que tous les services, les appareils et les logiciels sont sans cesse connectés à l'Internet.

Plus que jamais, les pirates informatiques possèdent à présent un motif pressant qui les amène à pénétrer les systèmes informatiques. Ce motif consiste à gagner de l'argent ou à exercer une extorsion ; ce motif peut également être politique ou économique.

Au cours des deux dernières décennies, des cyberattaques ont été menées contre l'infrastructure de tous les pays développés, infligeant de lourdes pertes à d'innombrables compagnies. Il est établi qu'il existe plus de 2000 cas confirmés de piratage de données chaque années, et que chacun d'eux coûte, à l'institution piratée, 3,9 millions de dollars en moyenne [26].

Bref, les piratages et les menaces sécuritaires ont un impact important sur presque n'importe quel système, dont les suivants :

- **Les communications:** les appels téléphoniques, les courriels, les SMS et les applications de correspondance peuvent être utilisés dans les cyberattaques.
- **Les affaires financières:** les institutions financières restent l'ultime cible des pirates. Idem pour toute autre institution qui traite ou entretient les informations de la banque ou de la carte de crédit.
- **Les gouvernements:** les institutions gouvernementales sont également le cible des pirates, surtout ceux qui cherchent à se procurer des informations privées des citoyens ou des données confidentielles.
- **Le transport:** les véhicules connectés au réseau Internet, les systèmes électroniques de l'organisation de la circulation et l'infrastructure des routes intelligentes sont tous sujets aux menaces cybernétiques.
- **La protection sanitaire :** toute ce qui a trait à la protection sanitaire, des registres des cliniques locales aux systèmes du traitement des cas d'urgence, sont sujets aux cyberattaques.
- **L'enseignement :** les institutions éducationnelles, leurs données confidentielles de recherche, et les informations qu'elles possèdent concernant les étudiants ou les employés, sont également sujets aux cyberattaques.

D'habitude, les sites web et les applications de YouTube sont les accès des pirates, puisqu'ils sont accessibles

via des connexions internet publiques et sont en général connectés à des Backend fragile, d'où la faiblesse de la stratégie sécuritaire de l'institution [27].

Les principes de la cybersécurité :

La cybersécurité vise en premier lieu à protéger les données. La sécurité en général repose sur trois principes ayant un rapport avec la sécurité des données et connus couramment sous le nom de « la Triade de la CIA » [28] :

- La confidentialité : c'est le fait de garantir l'accès aux données critiques, seulement des personnes qui ont en vraiment besoin. Ces personnes sont autorisées d'accéder à ces données, en vertu des politiques règlementaires.
- L'intégrité : c'est le fait de garantir que les données et les systèmes ne subissent ni une modification issue des mesures entreprises par les instances menacées, ni une modification occasionnelle. Par ailleurs, il faut prendre les mesures nécessaires pour entraver la corruption ou la perte des données délicates, et pour se rétablir rapidement au cas où cela se produirait.
- L'accès continu : c'est le fait de garder les données disponibles et utiles à leurs utilisateurs finaux, et d'éviter les obstacles qui peuvent empêcher cette disponibilité, comme les pannes, les cyberattaques ou les mesures sécuritaires elles-mêmes.

Le rôle de la cybersécurité dans la protection de l'industrie des jeux vidéo :

L'industrie des jeux vidéo constitue la plus grande industrie de divertissement dans le monde entier ; sa valeur sur le marché a dépassé les 197 milliards d'USD en 2022. La pandémie du Covid-19 a produit une croissance sensible de cette industrie, qui est arrivée à 26% en 2019 et en 2021. Le confinement total et la prévention de la mixité entre les membres de la société ont obligé les utilisateurs à vaquer aux jeux vidéo, leur seul refuge. Cette industrie croissante, qui entraîne l'échange des fonds et des données via Internet, a attiré les différents acteurs [29].

D'habitude, les joueurs placent leur confiance dans les jeux qui contiennent des informations personnelles privées, et y dépensent de l'argent réel ou codifié pour acheter les objets précieux dans le jeu. Ces données de valeur attirent les pirates pour s'en emparer. Ceux-ci possèdent des méthodes variées pour intercepter les données qui peuvent être revendues sur Internet ou qui aide à dévier l'argent des transactions vers leurs propres comptes.

Certains pirates cherchent les lacunes sécuritaires dans le jeu pour le figer. En fait, ces lacunes peuvent entraîner la rupture du service, ce qui nuit à la réputation de la compagnie productrice, et lui coûte de bonnes sommes d'argent.

C'est pourquoi il est impératif de respecter les protocole de la cybersécurité pour rester à l'abri du blocage des données, ou du vol lors des transactions dans le jeu, et pour prévenir les cyberattaques contre les logiciels des jeux, ou l'atteinte des appareils des utilisateurs par des virus malicieux.

Les menaces cybernétiques contre l'industrie des jeux vidéo :

Les menaces cybernétiques prennent des formes variées, en fonction des objectifs du pirate et des lacunes dans le logiciel du jeu. Parmi les menaces récurrentes qui gênent aux utilisateurs, figurent les suivants :

1- La modification du jeu :

C'est le fait d'intégrer des programmes importuns dans le jeu. Cette menace cybernétique est la plus fréquente qui attaque les petits jeux portables et, relativement, les jeux sur les ordinateurs Windows.

Les modifications appliquées requièrent, non seulement la connaissance du langage de programmation, mais surtout une connaissance spécialisée du cryptage, puisque le code source n'est généralement pas disponible. Ensuite, ces modifications sont vendues aux joueurs pour leur donner des avantages supplémentaires, surtout dans le jeux Internet à multi-joueurs. Parfois, les joueurs légitimes, se sentant vaincus à cause de ces modifications, abandonnent le jeu. De là, les développeurs des jeux vidéo doivent combler les lacunes, que les pirates peuvent exploiter pour effectuer des modifications. Si ces lacunes sont comblées, les pirates prendront longtemps pour créer des modifications rentables [30].

2- La fuite des informations personnelles d'identité :

La fuite des informations d'identification est une forme de cyberattaque, car les pirates compilent les informations personnelles de valeur pour les utiliser ou les vendre. La compilation de ces informations a lieu avec plusieurs méthodes : modifier les formulaires dans le jeu pour collecter des informations personnelles ; attaquer les entrepôts de données ; profiter des erreurs commises par les développeurs, susceptibles de dévoiler les données des utilisateurs... Les données compilées peuvent comprendre aussi des courriels, des

mots de passe, des informations de cartes de crédit ou de l'appareil, entre autres données personnelles et délicates.

Les jeux sur le téléphone portable constituent un attrait particulier pour la fuite des bases de données, car ces jeux collectent automatiquement souvent les données, sans avoir besoin de formulaires. Selon les études, 14% des applications IOS et Android qui utilisent le stockage en nuage sont susceptibles aux problèmes qui finissent par dévoiler les informations d'identification. En 2022, Neopets a révélé l'existence d'une violation de données qui a duré 18 mois, et qui a entraîné la fuite des informations personnelles de plus de 69 millions d'utilisateurs [31].

3- Les attaques d'hameçonnage :

Les attaques d'hameçonnage (phishing) visent à se procurer d'informations personnelles ou de paiements. Le pirate envoie à sa victime un message, feignant d'être envoyé de la part d'une personne fiable ou d'un service qui demande des informations personnelles. Dès que le pirate collecte ces informations, il le vend ou les utilise pour demander un rançon.

Les attaques d'hameçonnage sont les attaques les plus répandues, menées contre les joueurs. Au cours d'un seul et même année, un pare-feu a découvert plus de 3.1 millions de tentatives d'hameçonnage dans les jeux en ligne, qui ont toutes visé à se procurer des données d'identification de l'utilisateur pour s'emparer ses comptes des jeux. C'était le cas de jeux de renommée. Un site Web a été fondé pour présenter des prix dans le jeu, alors qu'il vise à collecter les données d'identification.

Souvent, les données d'identification dans les jeux comprennent aussi les informations du paiement, qui peuvent être plus tard volées. Si le joueur réécrit son mot de passe, le pirate peut utiliser les données d'dentification sur d'autres sites pour collecter davantage d'informations de valeur. En fait, les données d'identification sont un accès aux cyberattaques, puisque les données volées peuvent être utilisées pour violer d'autres systèmes [32].

4- Les attaques DDoS :

Les attaques par déni de service ou couramment les attaques DDoS visent à entraver le trafic ordinaire du serveur, ce qui ralentit ou bloque entièrement les connexions légitimes. Ces attaques peuvent exercer une pression sur les serveurs des jeux, ou empêchent la connexion de maints utilisateurs, ou ciblent les PC. Les motifs varient d'une attaque à l'autre, et requièrent chacun des données différentes.

Pour les individus, l'attaque DDoS ralentit le jeu en ligne ou le rend inopérant. En général, le motif de cette attaque est d'acquérir un avantage compétitif par rapport à l'utilisateur rival, en lui demandant son adresse IP ou en l'obtenant par des programmes malicieux. Lorsque ces attaques surviennent contre les jeux connectés à Internet, comme PlayStation Network ou Xbox Live, elles laissent les utilisateurs dans la déroute, incapables de jouer. En 2014, un groupe de pirates sont parvenus à fermer les réseaux de PlayStation et de Xbox [33].

5- Les malwares :

Certains jeux sur l'ordinateur et sur le téléphone portable représentent un danger qui menace la sécurité aussi bien des utilisateurs, à cause des pirates, que des développeurs. Les appareils peuvent être atteints de programmes malveillants (des malwares) qui visent à voler les données ; et ce, après le téléchargement d'un faux fichier ou d'un programme atteint d'un virus.

Parfois, les jeux sains, téléchargés sur Internet, peuvent être atteints de malwares, si un intrus y injecte des instructions informatiques nuisibles. Parfois encore, les pirates créent de fausses applications, qui ne sont que des virus, et cela est commun dans les téléchargements, effectués à partir de sites insécurisés. C'est le cas par exemple du jeu appelé « Minecraft », considéré comme l'un des jeux les plus atteints de malwares ; cela a été découvert lorsque l'on a détecté plus de 3 millions d'appareils, atteints de programmes malveillants entre les années 2020 et 2021 [34].

La protection des jeux vidéo contre les cyberattaques :

Les cyberattaques aboutissent lors des déficiences dans la cybersécurité des logiciels des jeux, ou lorsque les utilisateurs sont dupés pour fournir des informations de valeur. Les développeurs des jeux vidéo doivent prendre en compte l'importance de consolider la cybersécurité de ces logiciels et de la maintenir au fur et à mesure pour protéger les données des utilisateurs et garantir le fonctionnement du jeu comme prévu. L'intégration des protocoles de la cybersécurité dans tout le contenu du jeu et le contrôle de ses données réduisent les risques des cyberattaques réussies.

La construction du système de cybersécurité lors du développement du jeu :

La cybersécurité doit être l'une des priorités majeures à tenir en compte lors de la conception et de la construction des logiciels. Il faut à plusieurs reprises

revoir le code, examiner la conception, définir les éventuelles failles sécuritaires pour les pallier, avant d'écrire ou de produire les codes, et d'appliquer les meilleures pratiques pour développer le jeu, comme la modélisation de la menace, ou l'activation des analyses statiques des logiciels malveillants.

Contrôle du jeu lors du codage :

Les données de contrôle doivent être collectées du programme, puis les transformer en outil de contrôle pour repérer les problèmes cybernétiques. L'existence des alarmes dynamiques et d'une réaction automatique aux imprévus, les équipes compétentes peuvent réagir promptement aux cybermenaces et, par conséquent, réduire le nombre des utilisateurs affectés [35].

Procédés de l'authentification sécurisée :

Il faut vérifier que tous les mots de passe stockés sont protégés et chiffrés. De plus, l'authentification doit être sécurisée par le recours à plusieurs procédés, dont la vérification en deux étapes. Ces procédés sont un moyen de protection contre les cyberattaques, pour les raisons suivantes :

Une infrastructure sécurisée :

L'infrastructure des jeux contiennent les bases de données, les réseaux et les serveurs (en nuage ou locaux), lesquels activent les codes. En fait, les codes doivent recourir à des principes logiciels moins confiants, pour limiter le domaine des éventuelles attaques à travers les serveurs. Il faut placer les codes de protection contre les attaques DDoS sur les terminaux (endpoints), pour éviter d'interrompre l'expérience du jeu. Il faut vérifier que les bases de données sont chiffrées et sécurisées, surtout lors du stockage des données personnelles. Il faut enfin essayer, autant que faire se peut, d'emmagasiner les données sur plusieurs sites de stockage, de sorte à limiter le domaine des violations.

Les simulations des cyberattaques :

Les simulations d'attaques contre votre jeu aident à déterminer ses côtés vulnérables. Le test du stylo et le Red teaming (l'équipe de cyberadversaires) sont des services de simulation importants pour détecter et combler les lacunes sécuritaires lors du codage.

L'initiation des utilisateurs :

L'interaction avec les utilisateurs, autant que possible, est importante, pour les initier aux attaques d'hameçonnage et à la vérification l'authenticité des contacts, sur les données que votre jeu peut demander d'eux. Il faut également les mettre au courant, lorsque surviennent des tentatives d'hameçonnage, difficiles aux utilisateurs de détecter. Enfin, il faut conseiller les utilisateurs de créer des mots de passe forts, et d'éviter de répéter leur emploi dans les différents logiciels [36].

Références:

1- Al-Chahrouri, Maha Hosni (2008), Les jeux vidéo à l'époque de la mondialisation, leurs avantages et leurs inconvénients (en arabe), le Caire, Dar al-Maysarah, p. 26.

2- Al-Hamadâni, Chahbâ' Djâssim (2011), La relation entre la violence dans les jeux vidéo et le comportement agressif des élèves des écoles primaires, une thèse de magistère en arabe, Faculté de Pédagogie, Université de Tikrit, Iraq.

3- Abdel-Sâdiq, Adel (2015), Le cyberterrorisme, nouveau modèle et nouveaux défis (en arabe), Centre arabe des recherches sur le cyberespace, an 14 – Édition 52, p. 92.

4- Atiyah, Aysar Mohammad (2014), Le rôle des mécanismes de pointe dans la prévention des crimes modernes : le cyberterrorisme et les moyens de le juguler (en arabe), la Rencontre scientifique tenue sous le thème des « Crimes modernes à la lumière des mutations régionales et internationales », du 2 au 4 septembre 2014, Amman, Jordanie.

5- K. E. (2000). Video games and aggressive thoughts ،feelings ،and behaveior in the laboratory and in life. Journal of Personality and Social Psychology, 78.

6- The Effects of Vident Video Game Hdoits on Adolescent Hostility ،Aggressive Behaviors' ،and school performance ،Tourmal of Adolescence، 1) 27).

7- Al-Qillini, Fatma Youssef (1995), Les risques culturo-médiatiques que courent l'enfant : étude sur les effets négatifs de certains jeux modernes sur l'enfant égyptien (en arabe), la 3ème Conférence annuelle, tenue sous le thème de « L'enfant entre le danger et la toxicomanie', le Caire.
8- Baqlawah, Dalia Mahmoud (2009), Les jeux électroniques didactiques et leur rôle dans le développement de la pensée créative (en arabe), la conférence sur l'E-formation et le développement des ressources humaines, tenue au Caire les 12 et 13 août.
9- Anderson, C.A., ed (2004), Violent Video GfOQies: Specific Effects of Violent Content on Aggressive Thoughts and Behaviour, Advances in Experimental Social Psychology, 36.
10- Al-Saghîrî, Farîd (2013), Le jeu vidéo : une pratique des jeunes et son rapport avec la violence (en arabe), Revue Études et Recherches, Université al-Halifah, Algérie.
11- Spink B, A.K. McPherson (2006) Quantifying the Association Between Physical Activity and Injury in primary ; School-Aged children pediatrics, july1
12- Khalid Abdou al-Sarayrah (2008), Les E-publications et leur impact sur les librairies et les centres d'information, Oman, Kounouz al-Maarifah.
13- Peter Grabowski (2006), Les Cybercrimes : les dimensions mondiales des réseaux Internet et leurs effets socio-sécuritaires, Centre des Recherches et des Études sécuritaires, 6-8 novembre 2006, les EAU, première édition.
14- **https://globalriskinsights.com/2021/02/middle-east-the-resurgence-of-the-islamic-state-in-syria-and-iraq/**, février 2021.
15- Young Yi, Le terrorisme, les médias et la montée d'Internet, J.K. Molins, Prolon, 2016.
16- Ibid.
17- **https://www.justsecurity.org/75064/covid-19-and-terrorism-in-the-west-has-radicalization-really-gone-viral**2021 ,**/**
18- L'extrémisme de Jumanji : comment les jeux et la gamification peuvent faciliter l'extrémisme ?, Revue de la Déradicalisation, 2020
https://journals.sfu.ca/jd/index.php/jd/article/view/359/223
19- Twitch streamer Destiny perd son partenariat après son accusation « d'encourager la violence », Ginx, septembre 2020.
https://www.ginx.tv/en/twitch/twitch-streamer-destiny-loses-partnership-for-encouraging-violance-against-protesters
20- Comment le jeu « Call of Duty » (l'appel du devoir) devient un appel au Djihadisme ?, La sécurité intérieure aujourd'hui, août 2019
https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
21- L'extrémisme de Jumanji : comment les jeux et la gamification peuvent faciliter l'extrémisme ?, Revue de la Déradicalisation, 2020
https://journals.sfu.ca/jd/index.php/jd/article/view/359/223
22- Comment le jeu « Call of Duty » (l'appel du devoir) devient un appel au Djihadisme ?, La sécurité intérieure aujourd'hui, août 2019
https://www.hstoday.us/subject-matter-areas/counterterrorism/how-call-of-duty-is-transformed-into-a-call-for-jihad/
23- Ibid.
24- L'application Discord pour les discussions collectives dit avoir bloqué plus de 2000 communautés extrémistes, NPR, avril 2021
https://www.npr.org/2021/04/05/983855753/group-chat-app-discord-says-it-banned-more-than-2-000-extremist-communities?t=1617718575660
25- Statistiques de l'utilisation et de la croissance de Twitch : Combien de personnes utilisent Twitch en 2021 ?, BackLinko, janvier 2021
https://backlinko.com/twitch-users
26- What is Ethical (White Hat) Hacking | CEH Certification | Imperva
27-https://coralogix.com/blog/gaming-need-cyber-security/#:~:text=Cybersecurity%20protocols%20are%20necessary%20to,malware%20infections%20on%20users'%20devices
28-https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles#:~:text=These%20cyber%20security%20principles%20are,to%20identify%20cyber%20security%20incidents
29- À une Valeur de 175 milliards de dollars et une croissance de 19% en 2020 : les jeux vidéo, des gains par millions en faveur des compagnies et des joueurs, Portail du quotidien al-Ahram
بقيمة 175 مليار دولار ونمو 19% خلال 2020.. الألعاب الإلكترونية.. أرباح بالملايين للشركات واللاعبين - بوابة الأهرام (ahram.org.eg)
30- https://www.videogameschronicle.com/news/destiny-2-cheat-creator-agrees-to-pay-bungie-13-5-million-in-damages/
31- https://www.zimperium.com/blog/unsecured-cloud-configurations-exposing-information-in-thousands-of-mobile-apps/
32-https://securelist.com/gaming-related-cyberthreats-2021-2022/107346/#:~:text=One%20of%20the%20most%20widespread,account%20credentials%20or%20financial%20information
33- https://coralogix.com/blog/ddos-attack-political-cyber-attack/
34- https://vpnoverview.com/internet-safety/malware/malware-infected-games/
35- https://coralogix.com/blog/observability-security-work-together/
36- https://coralogix.com/blog/red-teaming-cybersecurity/