International journal of applied management and economics
Vol : 02 , N° 09 , Août 2024
ISSN : 2509-0720

Le Cyberterrorisme Est-Il Une Menace Réelle ?

Is Cyberterrorism A Real Threat ?

- **Auteur 1 :** BENRIDA Abdelaziz,
- **Auteur 2 :** BELGHITI Habiba,
- **Auteur 3 :** EL FISSI Chakib,

(1) : Doctorant à la Formation Doctorale : Droit public et politique, Structure de Recherche : Géopolitique et stratégie globale, Faculté des Sciences juridiques, économiques et sociales, Université Cadi Ayyad, Marrakech, Maroc

.

(2) : Enseignante-chercheuse, Département Droit Publique, Faculté des Sciences juridiques, économiques et sociales Marrakech, Université Cadi Ayyad, Marrakech, Maroc

.

(3) : Doctorant, Faculté des Sciences juridiques, économiques et sociales Mohammadia, Université Hassan II, Casablanca, Maroc

.

Conflit d'intérêts : L'auteur ne signale aucun conflit d'intérêts.

Pour citer cet article : BENRIDA .A, BELGHITI .H & EL FISSI .Ch (2024) « Le Cyberterrorisme Est-Il Une Menace Réelle ?»,

IJAME : Volume 02, N° 09 | Pp: 265– 280.

Date de soumission : Juillet 2024
Date de publication : Août 2024

DOI : 10.5281/zenodo.13696615

RÉSUMÉ

Le présent article procède à une revue des différentes perspectives sur le cyberterrorisme, soulignant la complexité du sujet et les divergences des opinions quant à la réalité de la menace cyberterroriste et mettant en évidence l'évolution de cette menace avec les avancées technologiques. L'approche constructiviste adoptée permet de comprendre les différentes perceptions de cette menace. Cependant que les avancées dans les technologies de l'information et des communications et la généralisation de leurs usages, augmentent les vulnérabilités des systèmes critiques et rendent la menace cyberterroriste réelle avec des conséquences graves.

Mots-clés :

Cyberterrorisme - cybersécurité – controverse conceptuelle - perception - menace cyberterroriste

ABSTRACT :

This article reviews the different perspectives on cyberterrorism, highlighting the complexity of the subject and the divergence of opinions on the reality of the cyberterrorist threat, and highlighting the evolution of this threat with technological advances. The constructivist approach adopted makes it possible to understand the different perceptions of this threat. However, advances in information and communication technologies and the generalization of their use increase the vulnerabilities of critical systems and make the cyberterrorist threat real with serious consequences.

Keywords:

Cyberterrorism - cybersecurity - conceptual controversy - perception - cyberterrorist threat

INTRODUCTION

La cybersécurité est un enjeu pour les États soucieux de préserver leurs organismes publics, leurs entreprises privées et leurs sociétés contre les cybermenaces et ce, de par l'augmentation du nombre des cyberattaques, de plus en plus perfectionnées. On compte parmi les cybermenaces la cyberguerre, le cyber espionnage, la cybercriminalité, le hacktivisme et le cyberterrorisme. Si les cybermenaces se distinguent les unes des autres par les mobiles de leurs auteurs, leurs modes d'action - les cyberattaques - se chevauchent voire, se confondent. Leurs auteurs sont pratiquement impossibles à démasquer. Les discours médiatiques et/ou politiques amplifient ou minimisent la gravité de ces cyberattaques. C'est dans cette toile de fond que le présent article examine la question de savoir si le cyberterrorisme constitue une menace réelle ou s'il reste principalement un concept théorique utilisé pour justifier des fins politiques et économiques.

Tenter de lever l'indétermination qui entoure la réalité de la menace cyberterroriste peut contribuer à une bonne préparation à faire face à des cyberattaques qui, de par leur gravité, sont susceptibles de menacer la sécurité nationale et internationale et la stabilité des Etats. Aussi, comprendre les conséquences économiques et sociales du cyberterrorisme aiderait les décideurs et les entreprises à mieux gérer les risques et à développer des plans de résilience et de continuité des activités surtout que le cyberterrorisme se confond facilement avec d'autre cybermenaces comme la cybercriminalité, la cyberguerre et la menace terroriste.

La problématique que soulève le présent article est relative à l'absence d'une définition universelle et claire du cyberterrorisme et ses implications au niveau de la perception de la menace. Les définitions varient selon les perceptions des chercheurs, des gouvernements et des organisations internationales. Certains considèrent toute utilisation d'Internet par des groupes terroristes comme du cyberterrorisme, tandis que d'autres limitent ce terme aux attaques visant le cyberespace dans ses différentes couches (matérielle, logique et sémantique). De cette ambiguïté découle un éventail de perceptions de la gravité de la menace voire sa réalité.

Pour traiter cette problématique, nous envisageons de répondre à ces trois questions :

- Quelle est la controverse conceptuelle entourant le concept de « cyberterrorisme » ?
- Quelles sont les différentes perceptions à propos des conséquences de la menace cyberterroriste induite par cette controverse ?
- Qu'est-ce qui rend ou pas, la menace cyberterroriste réelle ?

Cadre d'étude :

Cette problématique sera traitée dans le cadre du constructivisme qui puise sa genèse dans trois disciplines : philosophie, sociologie et psychologie. Et une de ses prémisses psychologique et sociologique est que « les individus agissent à l'égard d'autres individus et/ou objets en fonction des significations que ces individus et/ou objets revêtent pour eux »[1]. Ainsi, le constructivisme se base parmi autres sur la perception. Aussi, la menace est-elle une construction sociale et donc, une question aussi de perception. Plus particulièrement la théorie de sécuritisation de l'école de Copenhague constitue une approche possible pour s'expliquer les controverses qui entourent ce concept. La définition de la sécuritisation est donnée par Ole Wæver, un des précurseurs de la théorie de sécuritisation. Il considère la sécurité comme un acte de parole qui sécurise en considérant qu'un ou plusieurs objets référents comme menacés dans leur existence et qui doivent être protégés en urgence ; ce qui justifie la prise de mesures exceptionnelles[2]. Ainsi, la sécuritisation est un discours. Balzacq a donné une définition plus explicite de la sécuritisation. Pour lui, la sécuritisation est « un assemblage articulé de pratiques à travers lesquelles des artéfacts heuristiques (métaphores, instruments politiques, répertoires d'images, analogies, stéréotypes, émotions, etc.) sont contextuellement mobilisés par un acteur sécuritisateur qui incite l'audience à construire un réseau cohérent d'implications (sensations, pensées et intuitions), à propos de la vulnérabilité critique d'un objet de référence, lequel s'ajuste aux raisons de choix et d'actions de l'acteur sécuritisateur, en investissant le sujet de référence d'une aura menaçante, à un point tel qu'une politique ciblée va immédiatement être adoptée pour le bloquer »[3]. En explicitant les artéfacts heuristiques de sa définition susmentionné, Balzacq donne l'impression d'une perspective négative de la sécuritisation voire une manipulation de l'opinion publique. Pourtant, la sécuritisation n'est pas toujours négative. En effet, Balzac considère que la sécuritisation a, entre autres, pour conséquences : le secret, l'absence de transparence et les politiques d'exception. A contrario, « le risque débouche, quant à lui, sur une logique de précaution relayée par les mesures préventives, voire préemptives »[4]. Or, la menace est liée au risque car ce dernier est fonction de la probabilité de survenance d'un événement menaçant et de l'impact négatif potentiel si l'événement se produisait[5]. En

[1] Herbert Blumer cité par Balzacq, T. 2016. Chapitre 3 - Le Constructivisme. in *Théories de la sécurité : Les approches critiques*. Paris. Presses de Sciences Po, p. 172.
[2] Wæver, O. 1995. Securitization and Desecuritization. *On Security*, Ronnie D. Lipschutz, New York : Columbia University Press: p. 55
[3] Balzacq, *Op. cit. :* p. 194. C'est une définition que Balzacq avait donnée dans son ouvrage Securitization *Theory : How Security Problems Emerge and Dissolve.*
[4] *Ibid. p.214*
[5] NIST. 2012. *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30. Revision 1 : p. 12

considérant le principe de la précaution, Balzacq s'affranchit de la distinction entre la menace et le risque puisque « en cas de risque de dommages graves ou irréversibles, l'absence de certitude scientifique absolue ne doit pas servir de prétexte pour remettre à plus tard l'adoption de mesures effectives »[6]. Ainsi la sécuritisation du cyberterrorisme pourrait être un discours mais aussi, encore plus, une politique de précaution.

Cette approche nous a permis de formuler l'hypothèse selon laquelle la menace cyberterroriste est réelle ; ce qui justifie l'adoption de la sécuritisation.

Méthodologie.

La méthode appliquée est l'analyse comparative des définitions et des perceptions de la menace. Le présent article se décline en deux parties. La première traite des grandes lignes des débats relatifs à la controverse conceptuelle entourant la définition du cyberterrorisme. La deuxième partie est consacrée à l'évaluation de cette menace.

I — LE CYBERTERRORISME, UNE CONTROVERSE CONCEPTUELLE

Le vocable cyberterrorisme est relativement récent. Il a été inventé par Barry Collin, un chercheur à l'Institut de Sécurité et de Renseignement de Californie, au début des années 1980, en référence à la convergence du cyberespace et du terrorisme. Mais, depuis, les définitions de ce terme n'ont pas cessé de se multiplier. Elles sont à ce jour plus de 27 définitions. Or, « la définition a plusieurs fonctions. Elle sert à éclairer, à préciser, à lever les ambiguïtés, à expliquer, et créer un espace de discours commun »[7] ; ce qui n'est pas le cas pour le cyberterrorisme. Pour ce dernier, il y a deux catégories de définitions : celles restrictives qui stipulent que le cyberterrorisme se déroule entièrement dans le cyberespace. C'est le cyberterrorisme pur (1) et celles extensives qui définissent le cyberterrorisme par référence au terrorisme du monde réel. C'est le cyberterrorisme dit hybride (2).

1. Les définitions du cyberterrorisme pur

Les définitions restrictives encadrent le concept de cyberterrorisme dans des limites sans faire référence au terrorisme. Les plus répandues et par ordre chronologique sont les suivantes :

Barry Collin a défini, en 1997, le cyberterrorisme comme « la convergence de la cybernétique et du terrorisme » [8].

[6] Assemblée générale des Nations unies. 1992. ***Déclaration de RIO sur l'environnement et le développement***. *Principe 15*

[7] Loiseau, H. & Ventre, D. & Aden, H. 2021. Volume 3 : La cybersécurité en sciences humaines et sociales méthodologies de recherche. London. éditions ISTE. p. 35

[8] Krasavin, S. Ph.D. 2004. What is Cyber-terrorism ? . Computer Crime research Center. [Online] Available: https://www.crime-research.org/analytics/Krasavin/. (February 9, 2021)

S'inspirant d'une définition du Département de l'État des États-Unis en 1998, Mark Pollitt, agent spécial du *Federal Bureau of Investigation* des Etats-Unis d'Amérique, considère le cyberterrorisme comme « l'attaque préméditée et motivée par des considérations politiques contre l'information, les systèmes informatiques, les programmes informatiques et les données, qui entraîne la violence contre les cibles non engagées, par des groupes sub-nationaux ou des agents clandestins »[9]. Il précise cette définition en ajoutant que « pour que le cyberterrorisme ait un sens, nous devons être en mesure de le différencier d'autres types d'abus informatiques tels la criminalité informatique, l'espionnage économique ou la guerre de l'information » [10].

Pollitt considère que l'attaque se déroule totalement dans le cyberespace – dans ses trois couches, physique, logique et sémantique - avec des effets cependant sur les cibles civiles et ajoute deux éléments importants, la violence et la motivation d'ordre politique. Donc, Pollitt circonscrit l'action entièrement dans le cyberespace avec cependant des effets éventuels sur les cibles civiles.

En 2000, Dorothy Élisabeth Denning, dans une intervention devant la commission des services armés de la Chambre des représentants des États-Unis, affine davantage la définition de Pollitt et sort avec une définition, la plus citée par les chercheurs. En effet, pour Denning, « il s'agit d'attaques illégales contre des ordinateurs, des réseaux et des informations qui y sont stockées lorsqu'elles sont faites pour intimider ou contraindre un gouvernement ou son peuple dans le cadre d'objectifs politiques ou sociaux »[11]. Elle illustre sa définition par des exemples. Ainsi, Pour être qualifié de cyberterrorisme, une attaque doit entraîner la violence contre des personnes ou des biens, ou du moins causer suffisamment de torts pour susciter la peur. Les attaques qui entraînent la mort ou des blessures corporelles, les explosions et les écrasements d'avions, la contamination de l'eau ou des pertes économiques graves en seraient des exemples. Les attaques graves contre les infrastructures critiques pourraient être des actes de cyberterrorisme, en fonction de leur impact. Les attaques qui perturbent les services non essentiels ou qui sont principalement une nuisance coûteuse ne relèveraient pas du cyberterrorisme[12].

Quant à Gabriel Weimann, chercheur principal à l'Institut des États-Unis pour la paix et professeur de communication à l'Université de Haïfa, en Israël, il a défini en 2005, le

[9] Pollitt, M. M.1998. Cyberterrorism: Fact or Fancy . Computer Fraud & Security 2. p. 9
[10] *Ibid.*
[11] Denning, D. 2000. Cyberterrorism. [Online] Available: https://calhoun.nps.edu/server/api/core/bitstreams/5a802022-6ee1-427c-88d7-ccf4e670a2f3/content (August 28, 2024). Cet article est une extension du témoignage donné devant le Comité spécial de surveillance du terrorisme de la Commission des forces armées de la Chambre des représentants en mai 2000.
[12] *Denning. Op. cit.*

cyberterrorisme comme étant l'utilisation d'outils de réseau informatique pour nuire ou arrêter les infrastructures nationales critiques (telles que l'énergie, les transports, les opérations du gouvernement)[13]. Autrement dit, pour Weimann, le cyberterrorisme se déroule dans le cyberespace avec des conséquences dans le monde réel mais n'évoque pas la notion de violence ni celle de la motivation de l'action et ne dépasse pas la sphère des infrastructures critiques et les pouvoirs publics.

Enfin, en 2012, Jian Hua et Sanjay Bapna définissent le cyberterrorisme comme « une activité mise en œuvre par ordinateur, réseau, internet et informatique dans le but d'interférer dans le fonctionnement politique, social ou économique d'un groupe, d'une organisation ou d'un pays ; ou d'induire la violence physique ou la peur, motivés par les idéologies traditionnelles du terrorisme »[14]. Hua et Bapna élargissent les limites du cyberterrorisme pour englober le tissu économique du pays comme cible et font un lien avec les idéologies du terrorisme en ce qui concerne la motivation des actions.

In fine, toutes ces définitions ont en commun le fait que le cyberterrorisme se déroule dans le cyberespace avec des préjudices matériels ou corporels dans le monde réel. Par ailleurs, si le lien avec le terrorisme est pratiquement inexistant dans les définitions restrictives évoquées, il n'en est pas de même dans les définitions extensives qui insistent sur ce lien mais avec degrés différents.

2. Les définitions extensives ou le cyberterrorisme hybride

Certes, les définitions extensives considèrent qu'il y a un lien entre le cyberterrorisme et le terrorisme. Leurs approches incluent souvent d'autres formes d'utilisation terroriste d'Internet et pourraient donc définir le cyberterrorisme comme presque toute utilisation des technologies de l'information par les terroristes[15]. Mais, il y a là aussi des divergences des points de vue qui sont au nombre de quatre selon Lee Jarvis et Stuart Macdonald[16].

1er point de vue : Le cyberterrorisme est purement hypothétique ou improbable

À l'appui de ce point de vue, on trouve l'argument de James A. Lewis pour qui « les terroristes ou les armées étrangères peuvent bien lancer des cyberattaques, mais ils risquent d'être déçus de l'effet [car] … Les cyberattaques sont moins dommageables que les attaques physiques »[17].

[13] Weimann, G. 2005. Cyberterrorism: The Sum of all Fears?. Studies in Conflict & Terrorism. 28 : 2. p. 130
[14] Hua, J. & Bapna, S. 2012. How Can We Deter Cyber Terrorism?. Information Security Journal: A Global Perspective. 21: 2. p. 104.
[15] Jarvis, L. & Macdonald, S. 2015. What Is Cyberterrorism? Findings From a Survey of Researchers. Terrorism and Political Violence. 27:4. p. 659
[16] *Ibid.*
[17] Lewis, J. A. 2002. Assessing the Risks of Cyber Terrorism : Cyber War and Other Cyber Threats. Centre for Strategic and International Studies. Washington DC. 12. p. 11.

Une cyberattaque qui ne pourrait même pas être remarquée par ses victimes, ou attribuée à des retards de routine ou des pannes, ne sera pas l'arme que choisiraient les terroristes[18].

2e point de vue : le cyberterrorisme est une réalité mais qui est distincte des autres formes de terrorisme, exigeant sa propre définition

Ce point de vue est illustré par Thomas J. Holt qui considère qu'en dépit qu'il n'existe pas de définition unique convenue pour le cyberterrorisme, ce terme encapsule un large éventail de comportements autres que la terreur physique[19].

3e point de vue : le cyberterrorisme est un sous-ensemble du terrorisme qui est un concept plus large

Pour Michel Stohl, il faut « limiter le cyberterrorisme à des activités qui, en plus de leur composante cybernétique, ont des composantes communément convenues du terrorisme »[20], comme une certaine forme d'intimidation, de coercition, d'influence ainsi que de violence ou de menace ; ce qui le distinguerait de la cybercriminalité en se rapprochant de la définition de Pollitt suscitée qui exige le caractère violent.[21]

4e point de vue : le cyberterrorisme est un sous-ensemble du terrorisme, mais qu'il existe d'importantes différences qualitatives entre les deux

Ce point de vue allie entre le deuxième et troisième point de vue. Il est illustré par la définition de Laura Mayer Lux. Pour elle, « Pour que le cyberterrorisme soit effectivement une forme de terrorisme, il doit respecter la structure, le principe de préjudice et les éléments du terrorisme ».[22]

En ce qui concerne la structure, un acte cyberterroriste doit être un crime organisé par un collectif, ce qui exclue les cybercrimes individuels.[23] Pour le principe de préjudice, le cyberterrorisme s'attaque aux intérêts institutionnels, étatiques ou nationaux.[24] Enfin, pour ce qui est des éléments du terrorisme, il y en a deux : l'élément téléologique et l'élément instrumental. En ce qui concerne l'élément téléologique, « le cyberterrorisme doit être commis dans le but de modifier l'ordre constitutionnel ou de renverser le gouvernement légitimement

[18] *Ibid.* p.8
[19] Holt, T. J. 2012. Exploring the Intersections of Technology: Crime and Terror. Terrorism and Political Violence. 24. no. 2. 2012. p. 341.
[20] Stohl, M. 2006. Cyber Terrorism: A Clear and Present Danger. the Sum of All Fears. Breaking Point or Patriot Games? ». Crime. Law & Social Change. 46 : 223–238. p. 229.
[21] Jarvis, L. & Macdonald, S. Op.cit. p. 662
[22] Mayer. L. L. 2018. Defining Cyberterrorism. Revista Chilena de Derecho y Tecnologia. 7.2 : p.9.
[23] *Ibid.* p.14
[24] *Ibid.* p.15

élu. Par extension, le groupe cyberterroriste aura toujours un agenda politique » [25]. Enfin, pour l'élément instrumental, les actes cyberterroristes doivent induire chez le grand public l'incertitude « en établissant la croyance que n'importe qui, n'importe où, pourrait être victime de cyberterrorisme ».[26]

On peut donc, déduire que si les définitions restrictives et extensives du cyberterrorisme considèrent le cyberespace comme un outil, elles divergent quant à l'effet et à la cible de l'acte cyberterroriste. Pour les uns, le cyberespace est l'outil et la cible du cyberterrorisme - ce sont les auteurs des définitions restrictives ou encore le cyberterrorisme pur. Pour les autres, - ceux qui ont adopté les définitions extensives - il est l'outil. C'est ce qui est appelé le cyberterrorisme hybride par référence à la relation entre cyberterrorisme et terrorisme. De ce débat conceptuel, émerge naturellement la question légitime de savoir qu'elle est la réalité de la menace cyberterroriste.

II — LE CYBERTERRORISME EST-IL UNE MENACE RÉELLE

La différenciation dans la perception de la menace cyberterroriste interpelle les théories de « sécuritisation » et de « désécuritisation » de l'école de Copenhague. Ainsi, les États-Unis d'Amérique ont sécuritisé le cyberterrorisme depuis les attentats du 11 septembre 2001. A contrario, le cyberterrorisme a été désécuritisé par plusieurs autres auteurs en ne le considérant pas comme une menace existentielle.

La réalité de la menace (2) se trouve quelque part entre les perceptions minimalistes et maximalistes des effets du cyberterrorisme (1).

1. Le cyberterrorisme, une menace sous-dimensionnée

La menace du cyberterrorisme serait minime et donc, exagérée. Les auteurs de cette perception argumentent leur point de vue par la non-létalité de l'acte cyberterroriste. En effet, aucune victime n'a été l'objet de violence de la part de son ordinateur ou d'un réseau numérique. Pour d'autres, il y a certes des dégâts provoqués par des actes de cyberterrorisme mais, ces dégâts sont vite réparés si l'on dispose d'une stratégie de cyberrésilience. Il suffit d'avoir pris la précaution de disposer de sauvegardes pour se prémunir contre les ransomwares par exemple. En outre, elles ne touchent pas les infrastructures critiques qui travaillent en air gap[27]. Lorsqu'on n'est pas connecté à l'internet, on ne court aucun risque via le cyberespace.

Dans le cadre de cette perception, des acteurs politiques ou des médias peuvent être tentés de

[25] *Ibid.* p.16
[26] *Ibid.*
[27] C'est-à-dire travaillant avec des réseaux intranet

surdimensionner la menace pour des agendas qui leur sont propres. C'est ce qu'Olivier Kempf pense en considérant le cyberterrorisme comme un discours plus qu'une réalité[28]. Néanmoins, Kempf reconnaît la réalité de la menace cyberterroriste tout en minimisant ses effets violents dont le cyberterroriste peut s'en passer car il « n'a plus vraiment besoin de promouvoir son action grâce à la terreur et la disproportion entre des effets physiques et des effets psychologiques. Il réussit une œuvre psychologique directement, grâce au cyberespace. Son influence s'en trouve démultipliée » [29] donc sans violence. En effet, certes, le cyberespace est utilisé par les terroristes pour leur propagande, la transmission discrète de leurs messages et données pour la fabrication d'explosifs, ou pour se renseigner sur leurs cibles à dessein de s'informer sur leurs habitudes, ou pour les besoins de recrutement. Mais, « toutes ces techniques sont désormais à la portée de tous, qu'ils soient malfaisants ou non, terroristes ou non. Mafias, pirates, professionnels de l'intelligence économique, sociétés multinationales peu scrupuleuses (cela existe) ont le cyberespace à leur disposition pour préparer leurs actions, quelles qu'en soient les intentions » [30.]

Cet avis tranche avec ceux, comme James A. LEWIS, qui pensent que le cyberterrorisme existe mais il n'a pas le même effet psychologique que l'attaque physique. C'est un simple graffiti, sans réel effet dommageable, sauf s'il est entrepris pour renforcer une attaque physique. Lewis argumente son affirmation par une cyberattaque qui provoquerait la fermeture des vannes du système d'approvisionnement d'une ville en eau et qui ne peut être dommageable que si elle visait à priver les pompiers de s'approvisionner en eau au moment où une série d'incendies sont provoqués en parallèle[31]. Il ajoute aussi comme argument que les États-Unis ont utilisé des *brown-out* roulants pour tester les effets d'un arrêt du réseau électrique, sur la Californie. Les *brown-out* roulants n'ont pas mis la Californie à genoux[32]. Donc, la menace du cyberterrorisme serait simplement minime puisque les techniques utilisées sont à la portée de plusieurs cyber acteurs qu'ils soient terroristes ou non. Cette perception minimaliste tranche avec une autre, très alarmiste où la menace est peut-être surdimensionnée.

Dans le même sens, Norman E. Emery pense que les cyberattaques ou les attaques sur les réseaux informatiques sont des tactiques habilitantes qui peuvent améliorer l'impact d'un acte terroriste conventionnel, comme un attentat à la bombe. Elles seraient alors une tactique plutôt

[28] Kempf, O. 2014. Le cyberterrorisme : un discours plus qu'une réalité. Hérodote. La Découverte. 1 : 152-153.
[29] Kempf. *Op.cit.* p.94
[30] *Ibid.*
[31] Lewis, J. A. *Op.cit.* p.4
[32] *Ibid.*

qu'une catégorie à part du terrorisme.[33]

2. Le cyberterrorisme, une menace réelle non surdimensionnée

La menace du cyberterrorisme est prise avec sérieux par les États. Les conséquences potentielles des actes cyberterroristes pourraient être par exemple le dysfonctionnement des services ciblés, la déstabilisation des citoyens ou une situation de chaos dans la société[34]. Les scenarii potentiels sont nombreux, de plus en plus sophistiqués et dont certains sont plausibles au vu des défis rencontrés pour les contrer.

2.1 Les scenarii potentiels du cyberterrorisme sont nombreux :

Dans un article paru en 1997, Barry Colin avait prédit plusieurs scénarios potentiels très alarmistes du cyberterrorisme. Ainsi, à travers le cyberespace, un cyberterroriste n'a pas besoin d'être sur place, ou s'entourer d'une ceinture d'explosif ou monter dans un camion bourré d'explosif, pour perpétrer des actes terroristes. Il suffit par exemple, d'accéder aux systèmes de contrôle des usines pharmaceutiques pour modifier les dosages des médicaments, des banques centrales ou des bourses pour provoquer de graves dégâts. Le cyberterroriste fait arrêter les systèmes économiques d'une nation à partir d'un autre continent ; la déstabilisation sera alors réalisée.[35]

Plusieurs auteurs ont suggéré que les scenarii alarmistes ont seulement été exagérés par les médias et par les politiques. On peut citer parmi eux, Maura Conway, dans ses divers articles, Thomas RID pour lequel le nombre de cyberterroristes capables de mener des grands sabotages comme l'a été Stuxnet est très faible vu le niveau de sophistication requis[36] et Mark M. Pollit pour qui il y a suffisamment d'implication humaine dans les processus de contrôle utilisés aujourd'hui pour que le cyberterrorisme ne pose pas actuellement un risque significatif au sens classique du terme[37]. Si Pollit a minimisé les possibilités de survenue de ces scenarii, il a reconnu tout de même la nécessité d'une « approche proactive de la protection de l'infrastructure de l'information… pour éviter qu'elle ne devienne une vulnérabilité plus grave »[38]. Ainsi, plusieurs scenarii potentiels sont plausibles.

[33] Emery, N. E. 2005. The Myth of Cyberterrorism. Journal of Information Warfare. 4. 1: p.84.
[34] [n.a]. [n.d]. Cyberterrorisme : l'importance de la cybersécurité pour se protéger. Cyber Management School. [Online] available :https://www.cyber-management-school.com/ecole/les-fondamentaux-de-la-cybersecurite/cyberterrorisme-limportance-de-la-cybersecurite-pour-se-proteger/. (June 27, 2024).
[35] Collin, B. C. 1997. The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. 11th Annual international symposium on criminal justice issues. [Onlibne] available: https://www.crime-research.org/library/Cyberter .htm. (July 29, 2024).
[36] Rid, T. 2011. Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1): p.28.
[37] Denning, D. 2000, Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing. Chapiter Eight: Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation, 2001 :p.282
[38] Pollitt. *Op.cit.* p.10

2.2 Des scenarii potentiels plausibles :

- Le cyberterroriste pourrait piéger des bombes dans une ville par des systèmes informatiques qui communiqueraient entre eux de façon cryptée et qui exploseraient en même temps si l'une d'elles venait à être désamorcée. [39]
- Le cyberterroriste peut mettre en danger la sécurité publique en prenant le contrôle des systèmes de sécurité comme les caméras de surveillance ou l'éclairage public et mettre directement en danger la sécurité de la population.[40]
- Le cyberterrorisme vise à créer un climat de tension et de chaos en déstabilisant les citoyens et en érodant leur confiance dans les autorités ; ce que cherchent les acteurs du terrorisme conventionnel.
- Les cyberterroristes peuvent diffuser des fausses informations (Fake news et Deep fake) habilement conçus, sur les réseaux sociaux ou en directement par des SMS en se faisant passer pour des autorités afin de faire passer leurs messages et manipuler l'opinion publique et créer des troubles. Ainsi, il suffit de faire passer dans les réseaux sociaux l'éminence d'une attaque à la bombe lors d'un festival pour créer la débandade et le chaos avec indéniablement des victimes piétinées à mort ;
- Les cyberattaques contre des infrastructures de santé peuvent directement mettre en danger la vie des patients en perturbant les soins, en forçant, l'annulation d'interventions chirurgicales ou l'accès aux dossiers médicaux.

Ces scenarii sont plausibles car il y a des défis qui sont d'ordre technologique, juridique et politique, difficiles à relever.

2.3 Les défis

Les défis d'ordre technologique sont liés aux progrès des nouvelles technologiques de l'information, entre autres l'Intelligence Artificielle (IA), la généralisation de l'utilisation des objets connectés, l'industrie 4.0. En effet, les cyberterroristes peuvent exploiter les big datas par le recours à l'IA pour se renseigner sur les cibles potentielles, leur organisation, leurs vulnérabilités etc. En outre, l'IA pourrait être mise à profit pour mener des cyberattaques plus sophistiquées à grande échelle. Elle permet d'automatiser et d'optimiser les processus d'attaque en les rendant difficiles à détecter et à contrer rapidement.

[39] Collin, B. C. 1997. *Op. cit.*
[40] Datascientest. 2023. Quelles sont les conséquences d'une cyberattaque à l'échelle d'une commune ?. [Online] Available : https://www.lagazettedescommunes.com/857335/quelles-sont-les-consequences-dune-cyberattaque-a-lechelle-dune-commune/. (July 29, 2024)

Par ailleurs, le recours croissant à l'IA, l'industrie 4.0 et les objets connectés dans les systèmes d'information augmente en parallèle les vulnérabilités de ces systèmes qui peuvent être exploitées par les cyberterroristes.

Sur le registre juridique, la quasi-impossibilité d'attribuer des cyberattaques dans le cyberespace rend très difficile de démasquer les auteurs des cyberattaques pour les poursuivre vu le caractère transfrontalier de ces cyberattaques qui pourraient en plus, être des cybercrimes, du hacktivisme, de cyberguerre ou de cyberterrorisme de la part d'un individu, d'un groupe ou d'un État.

Enfin, sur le registre politique, la sécuritisation des réseaux sociaux et des médias électroniques se heurte à des considérations de liberté d'expression et des droits de l'homme. Dans leur lutte contre l'utilisation des réseaux sociaux et les médias pour la propagande des terroristes, les autorités américaines avaient demandé à *Twitter* (devenu ultérieurement X) de supprimer les messages incitant de propagande des terroristes. Mais elles ont reçu une réponse de non-recevoir car leur demande contrevient à la liberté d'expression défendue par le réseau social. Ainsi, *Twitter* avait répondu : « le terroriste d'un homme est le combattant de la liberté d'un autre ».[41]

Si ces défis rendent plusieurs scenarii plausibles, certaines cyberattaques ont ciblé des infrastructures vitales en provoquant des dégâts importants pouvant inspirer des cyberterroristes.

2.4 Des cyberattaques réelles aux dégâts graves

Des cyberattaques se sont produites aux États-Unis d'Amérique, au Costa Rica, et un peu partout dans le monde. Certes, ces attaques ont été considérées comme relevant de la cybercriminalité. Cependant, ce n'est pas parce que ces attaques ont utilisé un ransomware que les attaquants sont des cybercriminels et ce, d'autant plus que, l'attribution des attaques dans le cyberespace est pratiquement impossible.

Le 7 mai 2021, Colonial Pipeline a fait l'objet d'une cyberattaque par ransomware qui a obligé la Colonial Pipeline Company à cesser d'approvisionner ses clients. Elle a dû débourser la rançon de 4,4 millions dollars américains (USD) en bitcoin, dans les heures qui ont suivi l'attaque. Cependant le code fourni par les attaquants, a demandé un temps de traitement important pour restaurer le système. Donc, les dégâts financiers étaient importants. Le Colonial Pipeline, étant long de 5 500 miles, est considéré comme le plus grand pipeline de produits

[41] Chaffetz, J. and al. 2015. Radicalization: social media and the rise of terrorism. Washington, DC 20402-0001. Washington. DC 20402-0001. Committee on oversight and government reform :1-25

raffinés aux États-Unis.[42] L'attaque était une attaque informatique mais elle a paralysé le pipeline qui un système de technologie opérationnelle (OT). Or un système OT est beaucoup plus imposant que les systèmes informatiques des infrastructures critiques attaquables.[43]

En avril 2022, Gouvernement du Costa Rica a subi une cyberattaque par ransomware ayant provoqué des retards importants dans les opérations financières et administratives du pays et obligé le gouvernement décréter l'état d'urgence nationale et à refuser de payer la rançon de 10 millions USD ; ce qui a poussé les attaquants à lui réclamer 30 millions USD par jour de retard, au lieu de 10 millions USD.[44]

Si ces exemples concernent des dégâts purement financiers, d'autres peuvent avoir des conséquences aussi graves en perturbant par exemple le fonctionnement des hôpitaux comme en France, aux Royaume Uni. Par exemple, l'attaque du ransomware WannaCry en 2017, a affecté des systèmes d'information dans au moins 150 pays. En particulier, elle a touché des organisations critiques comme les services du Ministère de la santé publique et les hôpitaux du Royaume-Uni, des sociétés de télécommunications et autres dans le monde entier, qui ont été sujets à des perturbations généralisées et des pertes économiques importantes, voire sociales.[45]

[42] Grace, S. 2021. Cyberattack prompts major pipeline operator to halt operations. EDT / CBS News. [Online] Available : https://www.cbsnews.com/news/colonial-pipeline May 9. 2021 / 7:04 AM EDT / CBS News - cyberattack-shut-down/. (July 17, 2024). On pensait que le groupe de piratage cybercriminel qui serait basé en Russie se nommant DarkSide est celui qui a attaqué le Colonial Pipeline.

[43] Grace, S. *Op. cit*

[44] Fabien, T. 2024. Les plus grands syndicats de ransomware et comment ils fonctionnent. [Online] available: https://www.expressvpn.com/fr/blog/biggest-ransomware-syndicates-and-how-they-work/. (July 17, 2024)

[45] [n.a]. [n.d]. Les plus grands syndicats de ransomware et comment ils fonctionnent. ExpressVPN. [Online] Available : https://www.expressvpn.com/fr/blog/biggest-ransomware-syndicates-and-how-they-work/. (July 17, 2024)

CONCLUSION

Le débat sur le cyberterrorisme oscille entre ceux qui voient en lui une menace croissante et urgente et ceux qui considèrent que cette menace est surestimée. Les premiers mettent en avant la sophistication croissante des attaques et la dépendance accrue aux systèmes numériques, tandis que les seconds soulignent le manque de preuves empiriques et la complexité technique des cyberattaques réussies par des groupes terroristes.

Certes, les scenarii potentiels apparaissaient hypothétiques et peu probables car aucun de ces scenarii ne s'était produit avec des conséquences violentes et aussi graves que celles du terrorisme dans le monde réel. Toujours est-il qu'avec les prodigieuses avancées réalisées dans le domaine des technologies d'information et de communication telle l'intelligence artificielle, l'industrie 4.0 etc., et la généralisation de leurs usages dans la vie de tous les jours, par les citoyens, les villes intelligentes, dans les systèmes d'information de l'industrie, des infrastructures critiques, de la défense etc., les attaques cyberterroristes peuvent être graves. D'ailleurs, la montée en puissance de ces attaques et de leurs conséquences, a été prévue dès 2000, par Dorothy Denning à la Chambre des représentants des USA. Elle avait prédit que le cyberterrorisme violent ou aux conséquences graves, n'est qu'une question de temps car si les cyberterroristes - de l'époque - n'avaient pas l'expertise nécessaire, ceux qui grandiront dans la société de l'information pourraient disposer de cette expertise ou du moins, l'externaliser.[46] Le cyberterrorisme peut aussi faciliter ou amplifier des actes terroristes réels.

Donc, le cyberterrorisme, n'est ni un mythe instrumentalisé par les médias ou les entreprises de cybersécurité, ni un discours politique non fondé, mais bien une menace réelle qui suggère une sécuritisation active et proactive continuellement adaptée.

[46] Denning, D. 2000, Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing. Op.cit.

BIBLIOGRAPHIE

Assemblée générale des Nations unies. 1992. Déclaration de RIO sur l'environnement et le développement. Principe 15

Balzacq, T. 2016. Chapitre 3 - Le Constructivisme. in *Théories de la sécurité : Les approches critiques*. Paris. Presses de Sciences Po

Chaffetz, J. and al. 2015. Radicalization: social media and the rise of terrorism. Washington, DC 20402-0001. Washington. DC 20402-0001. Committee on oversight and government reform

Collin, B. C. 1997. The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge. 11th Annual international symposium on criminal justice issues. [Onlibne] available : https://www.crime-research.org/library/Cyberter .htm. (July 29, 2024).

Datascientest. 2023. Quelles sont les conséquences d'une cyberattaque à l'échelle d'une commune?. [Online] Available : https://www.lagazettedescommunes.com/857335/quelles-sont-les-consequences-dune-cyberattaque-a-lechelle-dune-commune/. (July 29, 2024)

Denning, D. 2000, Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing. Chapiter Eight: Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation, 2001 :239-288

Denning, D. 2000. Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism. Committee on Armed Services. U.S. House of Representatives. [On Line] available: https://henley-putnam.national.edu/wp-content/uploads/2016/12/Deterring-and-Dissuading-Cyberterrorism.pdf. (February 7, 2021).

Emery, N. E. 2005. The Myth of Cyberterrorism. Journal of Information Warfare. 4. 1: 80-89.

Fabien, T. 2024. Les plus grands syndicats de ransomware et comment ils fonctionnent. [Online] available: https://www.expressvpn.com/fr/blog/biggest-ransomware-syndicates-and-how-they-work/. (July 17, 2024)

Grace, S. 2021. Cyberattack prompts major pipeline operator to halt operations. EDT / CBS News. [Online] Available : https://www.cbsnews.com/news/colonial-pipeline May 9. 2021 / 7:04 AM EDT / CBS News -cyberattack-shut-down/. (July 17, 2024).

Holt, T. J. 2006. ''Exploring the Intersections of Technology. Crime. and Terror''. Terrorism and Political Violence. 24. no. 2. 2012. p. 341.

Hua, J. & Bapna, S. 2012. How Can We Deter Cyber Terrorism?. Information Security Journal: A Global Perspective. 21. 2: 102-114

Jarvis, L. & Macdonald, S. 2015. What Is Cyberterrorism? Findings From a Survey of

Researchers. Terrorism and Political Violence. 27. 4: 657-678

Kempf, O. 2014. Le cyberterrorisme : un discours plus qu'une réalité. Hérodote. La Découverte. 1 : 152-153.

Krasavin, S. Ph.D. 2004. What is Cyber-terrorism ? . Computer Crime research Center. [Online] Available: https://www.crime-research.org/analytics/Krasavin/. (February 9, 2021)

Lewis, J. A. 2002. Assessing the Risks of Cyber Terrorism : Cyber War and Other Cyber Threats. Centre for Strategic and International Studies. Washington DC. 12 : 1-12

Loiseau, H. & Ventre, D. & Aden, H. 2021. *Volume 3 : La cybersécurité en sciences humaines et sociales méthodologies de recherche*. London. éditions ISTE

Mayer. L. L. 2018. Defining Cyberterrorism. Revista Chilena de Derecho y Tecnologia. 7. 2 : 5–25.

NIST. 2012. *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30. Revision 1

Pollitt, M. M. 1998. Cyberterrorism — Fact or Fancy?. Computer Fraud & Security. 1998. 2: 8-10

Rid, T. 2011. Cyber War Will Not Take Place. Journal of Strategic Studies, 35. 1: 5–32.

Stohl, M. 2006. Cyber Terrorism: A Clear and Present Danger. the Sum of All Fears. Breaking Point or Patriot Games?. Crime. Law & Social Change. 46. 4-5 : 223-238.

Wæver, O. 1995. Securitization and Desecuritization. *On Security*, Ronnie D. Lipschutz, New York: Columbia University Press: 46-86.

Weimann, G. 2005. Cyberterrorism: The Sum of all Fears?. Studies in Conflict & Terrorism. 28. 2: 129-149

[n.a]. [n.d]. Cyberterrorisme : l'importance de la cybersécurité pour se protéger . Cyber Management School. [Online] available :https://www.cyber-management-school.com/ecole/les-fondamentaux-de-la-cybersecurite/cyberterrorisme-limportance-de-la-cybersecurite-pour-se-proteger/. (June 27, 2024).

[n.a]. [n.d]. Les plus grands syndicats de ransomware et comment ils fonctionnent. ExpressVPN. [Online] Available : https://www.expressvpn.com/fr/blog/biggest-ransomware-syndicates-and-how-they-work/. (July 17, 2024)