ИКОНОМИЧЕСКА МИСЪЛ
ECONOMIC THOUGHT

Икономическа мисъл / Economic Thought 68 (6) 2023

CYBER THREAT INTELLIGENCE. COMMENT METTRE EN PLACE UNE APPROCHE GLOBALE POUR LUTTER CONTRE LA MONTEE DES RISQUES INFORMATIQUES ?

Jean-François Rougé
Universités françaises

Как да се цитира тази статия / How to cite this article:

Rougé, J.-F. (2023). Cyber threat intelligence. Comment mettre en place une approche globale pour lutter contre la montée des risques informatiques ? (Cyber Threat Intelligence. How to Put in Place a Global Approach to Fight the Rise in It Risks?). *Economic Thought Journal*, 68 (6), 642-673 (*in French*). https://doi.org/10.56497/etj2368603

To link to this article / Връзка към статията:
https://etj.iki.bas.bg/other-special-topics/2024/03/13/cyber-threat-intelligence-comment-mettre-en-place-une-approche-globale-pour-lutter-contre-la-montee-des-risques-informatiques

Published online / Публикувана онлайн: 14 March 2024

CYBER THREAT INTELLIGENCE. COMMENT METTRE EN PLACE UNE APPROCHE GLOBALE POUR LUTTER CONTRE LA MONTEE DES RISQUES INFORMATIQUES ?

Jean-François Rougé

Universités françaises

Résumé : Le cyberespace est devenu l'un des champs de bataille de guerres qui ont d'ores et déjà changé l'ordre du monde. Faire face à ces menaces exige la mise en œuvre d'une intelligence des risques cyber. Elle se doit d'être globale, pluridisciplinaire et de toucher des acteurs de natures très différentes aux pouvoirs et aux capacités d'action disparates. Face à l'ampleur de la tâche cet article se pose la question : Comment mettre en place une approche globale pour lutter contre la montée des risques informatiques ? S'inspirant des pratiques de l'intelligence économique, il se propose d'y répondre à travers deux axes accessibles : Travailler à restreindre les sources humaines du risque cyber et préciser l'action publique pour le combattre.

Mots clés : Cybersécurité ; Cyber Threat Intelligence ; Cyberwarefaire ; Intelligence Economique ; Géostratégie ; Droit de l'informatique

JEL codes: B59

DOI: https://doi.org/10.56497/etj2368603

Received 16 October 2023

Revised 6 January 2024

Accepted 29 January2024

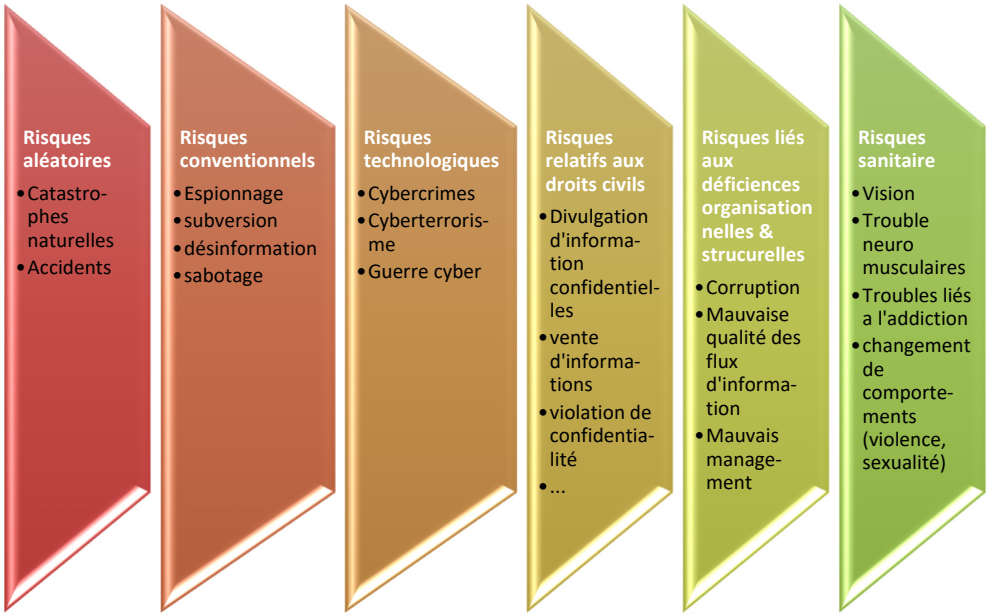
« *Nous assistons à un paradoxe : ce qui est complexe est simplifié par l'ignorance, ce qui devrait rester simple est complexifié par idéologie* »

Vincent Lavaux[1]

Le monde que nous connaissions change sous nos yeux ; vite, très vite.

[1] https://cercle-k2.fr/etudes/la-simplification-enjeu-democratique

Nous expliquions, il y a un peu plus de deux ans qu'Internet et son corollaire, le Cloud, étaient dangereux (Rougé, 2020). Sans même aborder les questions liées à leur perception, les risques cyber sont en effet tout aussi variés que nombreux :



Source : Gigerenzer 2004.

Figure 1. Nature des risques cyber

Depuis lors, le cyberespace est devenu l'un des champs de bataille ouvert de guerres (Cabriol, 2022)[2] qui ont d'ores et déjà changé l'ordre du monde. Il doit en découler une profonde modification de nos pratiques informatiques. Deux évènements ont joué un rôle prépondérant dans l'accélération et l'intensification de ces évolutions :

- La Covid d'une part, a nettement accéléré la mutation des organisations vers le Cloud afin de pallier les mesures sanitaires liées aux confinements. En parallèle, cette période s'est accompagnée d'un accroissement géométrique des attaques informatiques de toutes natures, contre les entreprises et les institutions publiques. Opérées tant par des Etats (espionnage & guerre cyber) que par des cyber criminels qui se sont clairement professionnalisés (Kshetri, 2010), ces agressions se sont généralisées. Rien n'est épargné, surtout pas les hôpitaux. Le coût économique en devient astronomique.

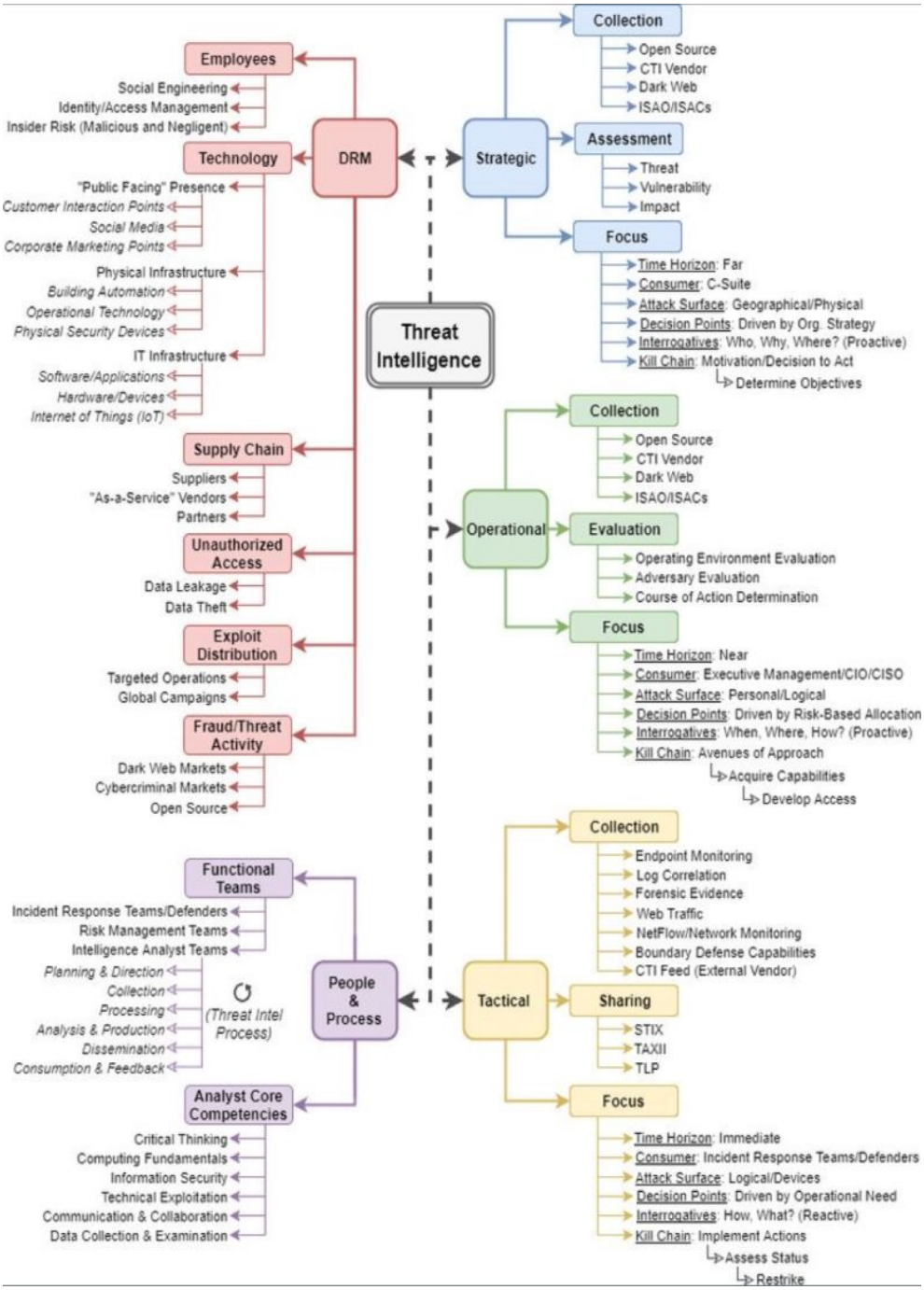
[2] De plus, le magazine télévisé « C dans l'air » (France 5) a consacré son numéro du 7 octobre 2022 à l'avènement de la cyber-guerre ; il note au passage la création, en Ukraine, de la première cyber-armée : l' Ukrainian Cyber Army. ; Voir également : (StealthLabs, 2020)

- La guerre en Ukraine a pour sa part, mis en lumière ce dont les stratèges militaires annonçaient depuis longtemps les prémices : l'utilisation d'Internet et du Cloud à des fins ouvertement offensives : la cyberwarefare (Mhalla, 2022). Les cyberattaques « sont des armes, en plus des armes traditionnelles » (Delville, 2022). Elle met en outre en lumière le danger vital que pose l'outsourcing à outrance des fonctions informatiques stratégiques. On savait depuis ses origines que l'outsourcing est une source majeure de cyber risque (Al Harrack, 2021) ; on n'avait pas imaginé les implications du fait de voir ses sous-traitants, quel qu'en soit le rang, tomber entre les mains ou sous l'influence de ses ennemis[3]. Elle met enfin en avant, ce que nous avait quelque peu fait oublier la mondialisation : l'importance de la géostratégie dans la sécurité (économique) des acteurs. A l'heure ou une nouvelle géopolitique se dessine sous nos yeux, quid du fait que la majeure partie de la sous-traitance informatique parfois à très haut niveau, se fasse dans les BRICS (où sous leur autorité) lesquels clament de plus en plus ouvertement leur indépendance, voir leur hostilité, face à l'occident ?

Alors que la cyber sécurité constitue un bien public de plus en plus évident (Karpiuk et Kostrubiec, 2022), ce tableau est déjà assez préoccupant. Suffisamment, en tous cas pour sortir la question de la maitrise des risques cyber de la sphère des spécialistes et justifier la mise en place, a l'instar de ce qui se fait en matière d'intelligence économique, de politiques « d'intelligence » des risques cyber, prenant en compte tous les niveaux de la société. Rappelons ici que « *l'intelligence économique peut être définie comme l'ensemble des actions de recherche, de traitement, de diffusion, de protection de l'information utile aux différents acteurs économiques. Ces acteurs sont conçus comme un système global destiné à inspirer la stratégie de la direction générale de l'entreprise tout comme à innerver ses différents niveaux d'exécution, afin de créer une gestion offensive et collective de l'information qui devient une richesse principale.* » (Martre, 1994).

Il importe en effet de prendre conscience que dans un système complexe tel l'espace cyber, « *relationships between several elements can lead to unpredictable instability* » (Helbing, 2013). Les éléments à prendre en compte sont ici très nombreux :

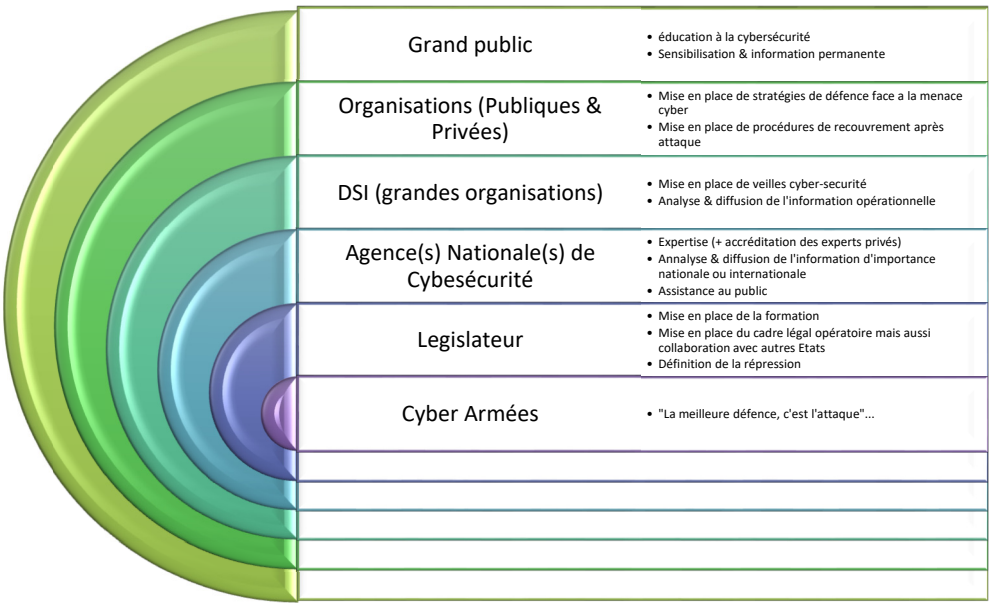
[3] Quel est le risque crée par un opérateur de call center travaillant chez un sous-traitant de 3° rang, menacé par une arme de guerre (lui ou sa famille laquelle peut être située dans une autre partie du globe) lorsqu'il a accès fusse de façon sécurisée aux Active Directory d'un système stratégique de l'organisation ? D'ores et déjà, The Economist du 6/10/2022 (https://www.economist.com/asia/2022/10/06/the-gangs-that-kidnap-asians-and-force-them-to-commit-cyberfraud?utm_medium=social-media.content.np&utm_source=facebook&utm_campaign=editorial-social&utm_content=discovery.content&fbclid=IwAR0mZ9JokD4S8w28-m2C9taJgA5AU28oC7Zz-NVd5QJwyMmQ-In7qjewZ5U) révèle que des gangs kidnappent des informaticiens pour les forcer à commettre des fraudes cybernétiques.



Source : https://lnkd.in/e-SYZ65f

Figure 2. Typologie de la Cyber Threat Intelligence

Sans même aborder pour le moment, la question de la guerre cyber (Richards, 2014) qui pousse la question de la sécurité à son paroxysme, la cyber threat intelligence se doit d'optimiser les synergies entre les trois catégories de parties prenantes à la sécurité de l'espace numérique. L'ordre étatique (international & national) y a bien sûr une place prépondérante tant sur le plan législatifs, qu'éducatif … et pénal. Mais son action n'a que peu de chance d'aboutir si elle n'est pas relayée par celle des organisations et surtout par le grand public : tant que des codes d'accès système sont inscrits sur un post-it collé sur l'écran, aucune précaution technique ou légale n'est utile. Le partage des tâches et responsabilités peut ainsi suivre le schéma suivant :



Source : Auteur

Figure 3. Acteurs de la Cyber Threat Intelligence

Les acteurs de la cyber threat intelligence ainsi définis, le processus de traitement pourrait intervenir selon le cycle « ADICPIRC » ci-dessous :

Source : Auteur.

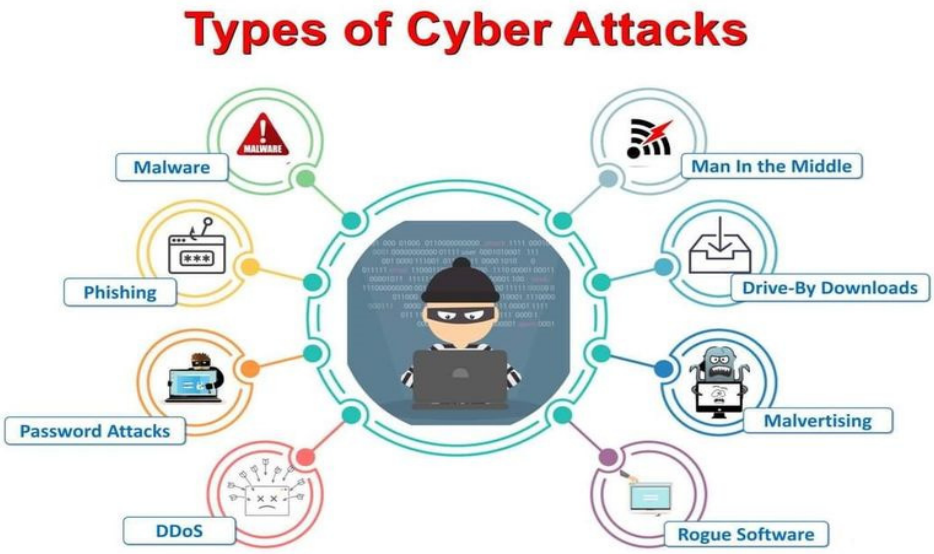
Figure 4. Procédure de traitement des risques cyber

Il ressort très nettement de ces divers graphiques que l'intelligence des risques cyber est une matière vitale, globale, pluridisciplinaire et qui touche des acteurs de natures très différentes aux pouvoirs et aux capacités d'action disparates.

La question se pose donc de la création d'une cyber Threat Intelligence. Plus précisément, « comment mettre en place une approche globale pour lutter contre la montée des risques informatiques ?» Face à l'impossibilité de donner une réponse exhaustive dans le cadre limité de cette analyse, nous faisons le choix de nous concentrer sur deux questions seulement dont le traitement contribue a minorer la criticité de ces risques : restreindre les sources humaines du risque cyber et analyse l'action publique pour le combattre[4].

Restreindre les sources humaines de cyber risques

Le constant est sans ambages : L'erreur humaine[5] est responsable de 90% des piratages informatiques [Altaya.com, 29/06/2022]. D'autre part, malgré la professionnalisation des attaques, les pirates informatiques assaillent le plus souvent les maillons les plus faibles de la sécurité, c'est le plus souvent l'utilisateur comme le démontre le schéma ci-dessous :



Source : https://ncsc.gov.uk

Figure 5. Typologie des Cyber Attaques

[4] Le lecteur intéressé par les questions purement techniques de cybersécurité pouvant se reporter aux nombreux ouvrages consacrés à la matière (Sikos et al., 2019; Loske, 2015; Jajodia, Kant et al., 2014; Bartsch et Frey, 2018).

[5] Dans les développements qui suivent l'erreur ne s'entend pas de la simple gaffe, mais comprend également l'erreur dolosive laquelle résulte d'une volonté de nuire.

Que ce soit grâce au phishing (très en vogue), à des les mots de passe non sécurisés ou à l'ouverture de fichiers corrompus, il représente la porte d'entrée la plus facile vers un système. En travaillant sur l'humain, on sécurise ainsi la première cible des attaques (Nicholson et al., 2016 & 2017) (Ahram et Nicholson, 2018). La question n'est pas facile, mais là encore l'intelligence économique nous donne des pistes d'action.

A cette fin, le triptyque classique former, informer, impliquer sera retenu pour essayer de proposer une approche globale d'amélioration du risque humain.

Former aux cyber risques

La position ici soutenue est que le meilleur moyen d'améliorer la situation en matière de cybersécurité afin d'augmenter la résilience des systèmes, est d'améliorer le niveau de compétence digitale des utilisateurs (Kaczmarek, 2022). Un bref voyage en amnésie, nous rappellera une époque où nous perdions facilement des heures, des jours ou plus de travail, pour n'avoir pas sauvegardé manuellement nos travaux, ou suite à une maladresse de manipulation de logiciels beaucoup moins conviviaux que les contemporains… L'apprentissage par l'erreur est toujours d'actualité en la matière, mais les erreurs des pionniers du PC ou de l'Internet, ne sont plus acceptables aujourd'hui. Au même titre que l'on forme les gens à l'informatique dès le plus jeune âge, il faut intégrer à ces formations les basics de la cybersécurité.

Pour confronter cette nécessité, depuis 2015, la commission européenne a mis en place des mesures visant à améliorer les connaissances digitales des citoyens européens. Ces efforts ont été inégalement relayées et/ou amplifiés par les Etats membres. Outre la disparité de résultats mis en lumière par Eurostat, il convient d'insister sur d'importantes divergences de situations en fonction des publics concernés :

- Au niveau pédagogique, la formation initiale des jeunes s'améliore (Pieczywok, 2022). Toutefois, outre les questions d'addiction, l'appétence digitale des jeunes est principalement tournée vers les réseaux sociaux. Ces derniers posent d'importants problèmes de confidentialité, de vols d'identité voire d'agressions (morales ou sexuelles notamment de pédopornographie). La situation reste donc délicate: d'autant que « *Contrary to popular belief that young people are the digital generation, study results have shown that a large part of this population have underdeveloped digital skills. Indeed, in all the studied countries, more than 15% of all students did not have adequate digital skills (European Commission, 2020). Moreover, according to OECD data, secondary school teachers in Europe rarely receive training in the use of ICT for educational purposes, and teachers themselves have voiced their need to develop*

professionally in terms of ICT skills (Europa Nu, 2021). » (Kaczmarek, 2022, 34) Elle inquiète d'autant plus qu'une étude de montre que l'indifférence à la cybersécurité touche également des étudiants du supérieur de la Silicon Valley (Moallem, 2018, 79) (Ahram et Nicholson, 2018).

- Au niveau andragogique, ces efforts ont encore plus de difficultés à atteindre leurs objectifs : « *In 2019, a total of more than 75 million working-age adults in Europe did not have at least basic digital skills. This mostly included the elderly, the undereducated and the unemployed. Meanwhile, more than 90% of jobs already require at least basic digital skills*. » (Kaczmarek, 2022, 32).

Alors même que le monde contemporain demande le développement de l'esprit critique et une capacité toujours affinée à vérifier ses informations, il est vrai que nombre des systèmes scolaire, même des plus avancés (The Economist, 2022), peinent déjà à enseigner comment lire, écrire et calculer… Face à ces résultats choquants, on ne peut qu'insister sur la nécessité d'inscrire les questions de cybersécurité dans l'apprentissage des compétences de (digitales) de base. Il y va de la sécurité nationale. A défaut de faire leur travail, il faut dire qu'ils manquent eux même de moyens tant humains surtout que techniques, les systèmes éducatifs doivent à minima inciter les gens à s'auto former et promouvoir les moyens alternatifs, tels les nombreux MOOC de vulgarisation à la cyber sécurité. Les formations en ligne dispensées par les agences nationales de sécurité informatique (USA & Europe) sont ainsi tout à la fois très bien faites et très pédagogiques.

Le principal objectif de ces formations est indiscutablement de créer une prise de consciences de masse des risques liés à l'utilisation quotidienne des TIC. Il serait bon qu'elles ouvrent sur une compréhension généralisée des grands traits concernant les méthodes utilisées par les attaquants tout en constituant, si possible un terreau pour développer de réelles connaissances techniques en cybersécurité. Malheureusement, pour compliquer les choses, la matière est très évolutive. Indispensables ces premiers efforts doivent être accompagnés d'une information permanente.

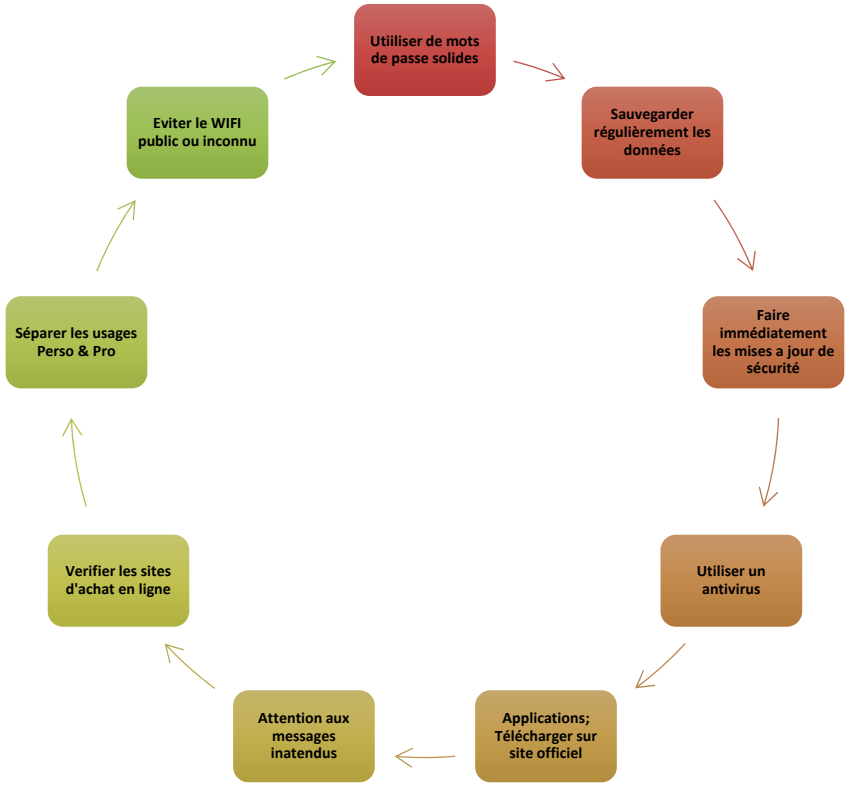
Informer sur l'actualité des cyber risques

La recherche insiste sur le fait qu'il n'existe aucun outil susceptible de prévenir les manipulations ou la désinformation qui sont à la base de la majorité des cyber dangers. Ce qu'un utilisateur peut faire pour se protéger des risques cyber dépend donc principalement de sa conscience et de sa connaissance ainsi que de son appétence aux risques (Moallem, 2018 ; Loske, 2015).

Eu égard à la complexité et variabilité des formes de cyber menaces, une fois la formation initiale à la cyber sécurité effectuée, l'information sur l'évolution des types

de menaces doit être tout à la fois régulière et surtout compréhensible par les non informaticiens. Le partage d'informations pertinentes, ciblées et pédagogiques est donc un élément essentiel de la cyber threat intelligence. Il implique la consolidation et la standardisation des informations concernant les risques cyber (Ferens, 2021).

Par défaut, il faut rabâcher les 10 mesures essentielles pour assurer sa sécurité numérique selon Cybermalveillance France[6]:



Source : https://cybermalveillance.gouv.fr

Figure 6. Les basics de la cybersécurité

Face à la professionnalisation des cyber attaquants, qui vont jusqu'à proposer des services de hacking pour les nuls, sur abonnement[7], l'information doit être tournée vers l'appréhension et l'appétence aux risques cyber des utilisateurs Lambda (Les

[6] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

[7] https://www.journaldunet.com/solutions/dsi/1515639-evilproxy-un-service-de-hacking-sur-abonnement/

professionnels de l'informatique étant sensés se tenir informés). L'information existe, elle est souvent gratuite, pédagogique et de bonne qualité[8]. Même si de très bonnes sources privées existent, on ne peut que recommander de suivre les agences nationales de cybersécurité :

- https://dgssi.gov.ma
- https://cybermalveillance.gouv.fr
- https://ssi.gouv.fr
- https://ncsc.gov.uk
- https://cisa.gov (USA)

Pour favoriser l'abonnement à ces sites, ou du moins aux alertes qu'ils diffusent quelques moyens simples peuvent être suggérés :

- A l'image de ce qui est fait en matière de sécurité routière, il serait souhaitable d'utiliser les médias grand public pour diffuser très régulièrement des clips d'informations sur les comportements à risque.
- La communication sur les efforts faits par les agences nationales de cybersécurité pour former et informer souvent en temps réel, les particuliers et les PME/PMI, doit être plus systématique. Des négociations avec les grands éditeurs de navigateurs Internet permettrait une connaissance beaucoup plus large de ces agences et de leur travail

Encore cette information demande-t-elle une proactivité des utilisateurs et le fait d'y consacrer un peu de temps. Ni l'une, ni l'autre ne vont de soit dans le monde contemporain. Aussi peut il être intéressant d'utiliser des mesures d'incitation.

Impliquer l'utilisateur dans la cybersécurité

La cyber threat intelligence est l'affaire de tous ; elle augmente le niveau de sécurité de systèmes qui sont vitaux pour nos modes de vie contemporains. La difficulté est qu'elle est contraignante. Outre les efforts permanents de formation et d'information qu'elle demande, la cybersécurité se traduit par des contraintes parfois très lourdes qui pèsent sur les utilisateurs. La tentation est grande de d'éluder les règles de sécurité. Afin de palier ce risque, trois méthodes peuvent être utilisées : Travailler sur l'ergonomie de la sécurité ; Inciter les comportements appropriés ; Contraindre les comportements déviants.

[8] Pour exemple le document : https://www.ssi.gouv.fr/uploads/2022/09/anssi-cybermois_2020-bd-cyber pirates.pdf

L'ergonomie de la cybersécurité

C'est un point capital. Il fait la fortune des sociétés de support technique informatique dans lesquelles la majorité des appels facturées se font sur la base d'une difficulté de connexion dues le plus souvent au paramétrage des logiciels de sécurité, d'identification (multiples), d'accès à Azure, AWS et autres Zscaler… Indispensables, les Identity Access Management, Privilege Access Management et autres doivent se faire de la façon la plus transparente possible pour l'utilisateur.

- Comment concilier la nécessité de procédures d'identification sécurisées avec l'incapacité à retenir de multiples mots de passe forts qui, de plus, doivent être changés régulièrement et n'ont plus aucun sens littéral pour l'utilisateur (Exemple de MP fort à ce jour : W54#ycZ861xU@gd7)?
- Quelles procédures alternatives peut-on adopter (Chmielewski, 2022):
    - Reconnaissance biométrique simple ou multiple (Obaidat, et al. 2019) ?;
    - Reconnaissance graphique ?
    - Procédé externe (clé sécurisée à lecteur biométrique…) ?

Les enjeux de l'ergonomie des systèmes de cybersécurité sont donc capitaux si l'on veut que les utilisateurs les emploient. On peut également les y inciter de façon plus ou moins contraignante.

Inciter les utilisateurs à respecter les règles de cybersécurité

L'incitation peut prendre des formes multiples et complémentaires.

- Tout d'abord, il est possible d'intégrer les concepts de cybersécurité dans des cursus d'apprentissages (IT ou non ; initiaux ou continus) en leur y adjoignant un bénéfice (Azzeh, Altamimi et Atallah Aloudat, 2022).
- Une forme de « discrimination positive » peut être affichée dans des processus comme le recrutement, la promotion ou la mutation.
- La rétribution sous forme de reconnaissance publique (certificats, prix, simples félicitations publiques …) peut utilement compléter une incitation pécuniaire aux efforts en matière de cybersécurité

La sociologie et la psychologie étudient beaucoup mieux qu'il ne nous est possible de le faire, comment motiver les comportements. Le point important à préciser est que ces disciplines font partie intégrante d'un développement d'une Intelligence des risques informatiques. Ces mêmes professionnels sont d'ailleurs les premiers à suggérer que quand l'incitation ne suffit pas, il peut être utile d'utiliser une forme de contrainte.

Contraindre les utilisateurs à respecter les règles de cybersécurité

Cette contrainte peut être plus ou moins sévère et prendre divers aspects. La mise en place de processus techniques (identifications multiples) permettant d'avoir accès aux systèmes ne sera pas abordée ici. Délibérément, ce paragraphe se concentrera sur les moyens managériaux utiles à renforcer la cybersécurité.

Au regard du droit du travail tel que défini par l'organisation Internationale du Travail (Hepple 2005), les employeurs disposent d'outils très efficaces à ces fins : le contrat de travail et/ou règlement d'entreprise.

- Le contrat de travail est l'acte juridique qui crée le lien de subordination entre un employeur et un employé. Dans la mesure où il respecte les règles légales, il a donc vocation à créer les conditions de cette subordination. Ainsi peut-il comprendre des clauses relatives à la cybersécurité. Elles peuvent être intégrées soit dans le corps du contrat soit par un avenant lié au contrat de travail. Dans les deux cas, elles sont contraignantes et susceptibles de sanctions prévues au contrat.
- Le règlement d'entreprise est quant à lui un acte unilatéral de l'employeur pour organiser les règles de vie, d'hygiène et de sécurité dans l'entreprise. Bien qu'il ne soit pas toujours obligatoire[9], et qu'il entraine souvent des contraintes administratives[10], l'usage de ce document est vivement recommandé. Des dispositions relatives à la cybersécurité peuvent dès lors être prises dans cet acte, susceptibles d'entrainer des sanctions qu'il précise.

Une utilisation judicieuse de ces instruments permet donc d'accroitre sensiblement le niveau de cybersécurité des organisations.

Au terme de cette première section, il est clair que la mise en œuvre d'une Intelligence des risques cyber, passe par un très gros travail sur la question des individus qui utilisent les TIC. Tout aussi ardue que capitale, ce pan de la matière fait appel à des disciplines très diverses qui n'ont que peu l'habitude de travailler de commun : droit, économie, sociologie, psychologie, mathématiques, théories des risques… On en oublierait presque que l'on parle de Technologies de l'Information et des communications !

[9] En ce qui concerne le droit du travail français, il ne l'impose que dans les entreprises de plus de 20 personnes.

[10] Toujours dans le cas français, outre sa rédaction par l'employeur, la mise en place du règlement intérieur entraine la consultation des représentants du personnel, sa communication à l'inspection du travail dont dépend le siège de l'entreprise, son dépôt auprès du tribunal des prud'hommes et sa diffusion auprès des salariés.

Tel sera également le cas dans notre seconde section consacrée au rôle des autorités publiques dans la mise en œuvre de la cyber threat Intelligence.

Sécuriser l'environnement dans lequel se déploie le cyberespace

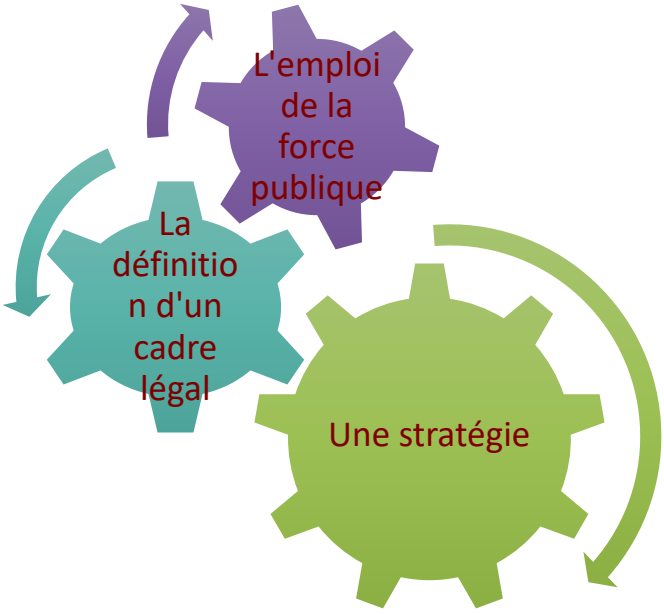
Les principaux régulateurs, les Etats et les institutions internationales ont un rôle majeur à jouer comme source de cybersécurité à travers la mise en place de politique et de législations appropriées tant à maintenir la confiance dans l'économie numérique, qu'à sanctionner les atteintes au fonctionnement du cyberespace (Pilzo, 2022). Mais pour y parvenir, des stratégies doivent d'abord être définie. Comme ce qui ce fait en matière d'intelligence économique (qui nous sert de cadre d'inspiration), la mise en place d'une cyber threat intelligence leur fait une place prépondérante. Il leur appartient de créer un « écosystème » (formation, information, stimulation), de le réglementer et d'en assurer la sécurité (passivement : veille, normes de résilience ; activement ; cyber vigilance, attaque (préventive)).

Sans en réfuter ni la pertinence, ni l'importance, nous ne pensons pas qu'il soit possible de limiter l'action étatique en la matière aux 5 composants d'une stratégie de cybersécurité efficace énoncées par (Fadia, Nayfeh et Noble, 2020):

Source : Fadia, Nayfeh et Noble, 2020.

Figure 7. Composants d'une stratégie de cybersécurité

Aussi préfèrerons nous une approche basée sur les axes suivants :



Source : Auteur.

Figure 8. Stratégie publique de cybersécurité

De la cybersécurité à la Cyber Threat Intelligence : la stratégie

« *L'hétérogénéité des cadres juridiques, l'absence de stratégies nationales, les capacités limitées de la justice pénale à lutter contre la cybercriminalité et à sécuriser les preuves électroniques, ainsi que les infrastructures d'information encore peu sécurisées dans un certain nombre de pays, font des sociétés du monde entier des cibles vulnérables à la cybercriminalité. En outre, les gouvernements ont du mal à concilier des réponses efficaces à la cybercriminalité avec les exigences des droits de l'homme et de l'État de droit en ligne*. »[11]. Alors que certains cherchent déjà à définir une éthique de la cybersécurité (Kizza 2014), voire de la cyberguerre (Taddeo, Glorioso et al., 2017) (Allhoff, Henschke et al., 2016), les questions s'enchainent plus vite que les réponses face à la croissance de la cyber insécurité.

Nul n'est donc besoin d'insister sur le côté indispensable de la définition de stratégies avant d'agir. Plus intéressant est de s'interroger sur le cadre de la détermination de cette stratégie. En l'espèce, Internet et le Cyber espace. Le problème ici est que nous avons à faire à un espace certes pleins de promesses et de dangers, mais virtuel ; non territorialisé. Or les Etats et leurs pouvoirs sont définis par un territoire géographique. Pour tenir compte de cette dichotomie, la stratégie définie doit être déterminée au

[11] https://www.pgaction.org/fr/ips/cybersecurity.html

deux niveaux de la dimension étatique : personne morale de droit international & souverain sur son territoire.

La composante internationale des stratégies étatiques d'Intelligence des risques cyber

A défaut de pouvoir localiser nombre des informations utilisées dans le cyber espace, les Etats doivent coopérer pour assurer la cyber sécurité (Skopick, 2018). La chose était déjà très délicate, au vu de leurs intérêts divergents (Eriksson, Giacomello et al., 2007). Elle se complique singulièrement avec la réapparition des frontières induites par la covid et la guerre en Ukraine. Il est déjà acté en cette fin d'année 2022, que le monde a changé irrémédiablement ; les frontières réapparaissent induisant la renaissance de la géopolitique et de la géostratégie. En effet, comment continuer à stocker ses informations et surtout, à les faires traiter, à ouvrir le coeur des ses systèmes d'information stratégique (Cloud)… dans des pays qui s'inscrivent ouvertement en confrontation avec vos valeurs fondamentales (Occident vs BRICS élargis) ? La nécessité d'une stratégie pour renforcer la création d'un véritable « droit public international du cyberespace » ne fait que s'accentuer (Kittichaisaree, 2017).

La question dépasse largement le cauchemar des seuls directeurs de la sécurité informatique des multinationales ou de des responsables de PME/PMI de secteurs sensibles, utilisant le Cloud as a Service ! « *Il est devenu essentiel de développer des mesures techniques et non techniques permettant aux États et aux entreprises de se protéger et de se défendre dans ce nouvel espace souvent considéré comme le cinquième champ de conflictualité après la terre, la mer, l'air et l'espace extra-atmosphérique*. » (Barat-Ginies, 2014). Tout comme l'ONU propose de « gérer la cyberguerre par la coopération internationale » (Taliharn), la cybersécurité devenue bien public universel, ne peut l'être que de la même façon. Problème : l'ordre international établi semble vaciller très rapidement ; Nul, à ce jour, ne peut dire sur quelles bases et quand il pourra être rétabli alors que « *Les domaines, comme le partage de l'information et du renseignement et l'aide mutuelle, peuvent devenir essentiels pour gérer une cybercrise, mais l'efficacité d'une telle coopération dépend considérablement de la cohérence des objectifs politiques et des relations bilatérales et multilatérales*. » (Taliharn). Or comme le remarque très justement le magazine Numérama du 2/11/2022 : « les hackers criminels russes peuvent être tranquilles, Moscou ne les arrêtera jamais ».

Alors que l'ordre international multilatéral pose problème dans la définition d'une stratégie globale de lutte contre la cyber-insécurité, tel n'est pas le cas, bien au contraire de l'ordre international régional. A ce niveau, force est de constater que l'Europe se montre, pour une fois, exemplaire avec la définition, dès 2001 d'une stratégie de cybersécurité européenne (CE Bucarest) ; suivie, entre autre par une stratégie globale de protection des données en 2016 (Voig, dem et al., 2017) ou de la toute récente « Législation sur les services numériques » d'avril 2022.

A défaut d'être complète cette stratégie internationale existe au niveau régional. Par exemple, le Conseil de l'Europe a défini une politique de « lutte contre les cybermenaces » très claire[12].

Les composantes nationales des stratégies étatiques d'Intelligence des risques cyber

« Les Etats n'ont pas d'amis, ils n'ont que des intérêts » (C. de Gaulle), il leur appartient donc de le préserver en mettant en œuvre les moyens nécessaires. Dans le cadre des relations internationales régionales, une partie de la définition de ces moyens découle d'une norme internationale. Tel est le cas en Europe, ou la convention de Bucarest 2001 impose à minima aux Etats membres : un organe national de cybersécurité ; un programme national de protection des infrastructures critiques, une planification de restauration après attaque. Force est de constater que ces dispositions, malgré leur indéniable intérêt, sont très défensives.

C'est la raison pour laquelle nous recommandons la mise en place d'une Intelligence des Risques Cyber, qui non seulement coordonnerait les choses entre les moyens existants, mais en plus définirait clairement tant les objectifs de cybersécurité à atteindre qui la façon d'impliquer tous les membres de la population dans ces objectifs. Au passage, la définition d'une telle stratégie, définirait une approche beaucoup plus proactive face aux risques cyber ; une fois attaqué, ont à déjà perdu ! Au moins une bataille. La question se pose enfin de la création d'une cyber armée et de sa coordination avec les agences de cyber sécurité.

Dans un état de droit, lorsque les options stratégiques sont définies, il reste à instaurer le cadre juridique qui les encadre et sanctionne leur non respect. Ce n'est pas le plus simple.

De la cybersécurité à la Cyber Threat Intelligence : la définition d'un cadre légal

La mise en place de régulations étatiques est fondamentale en matière de cybersécurité (Tyrawa, 2022). Une réponse légale doit assurer tout à la fois la qualification légale et la réponse adéquate aux attaques informatiques (Czuryk, 2022). La protection légale concerne une situation globale qui inclue plusieurs niveaux ; les organisations, en commençant par l'Etat et ses institutions, pour s'étendre aux individus en tant qu'acteurs au sein de diverses organisations, mais aussi que personnes disposant de droits spécifiques quant à leur vie privée et leurs informations (data). Il en découle l'utilisation plusieurs techniques juridiques qui vont des plus contraignantes, aux simples recommandations en passant bien sûr par la répression des pratiques désapprouvées.

[12] https://www.consilium.europa.eu/fr/policies/cybersecurity/

Source : Auteur.

Figure 9. Pourquoi utiliser la loi en matière de cybersécurité

Alors que l'inflation législative (qui mine tant la sécurité juridique que la confiance dans de nombreux pays) pourrait laisser, qu'« une loi de plus » n'est qu'une formalité, plusieurs obstacles viennent compliquer les choses :

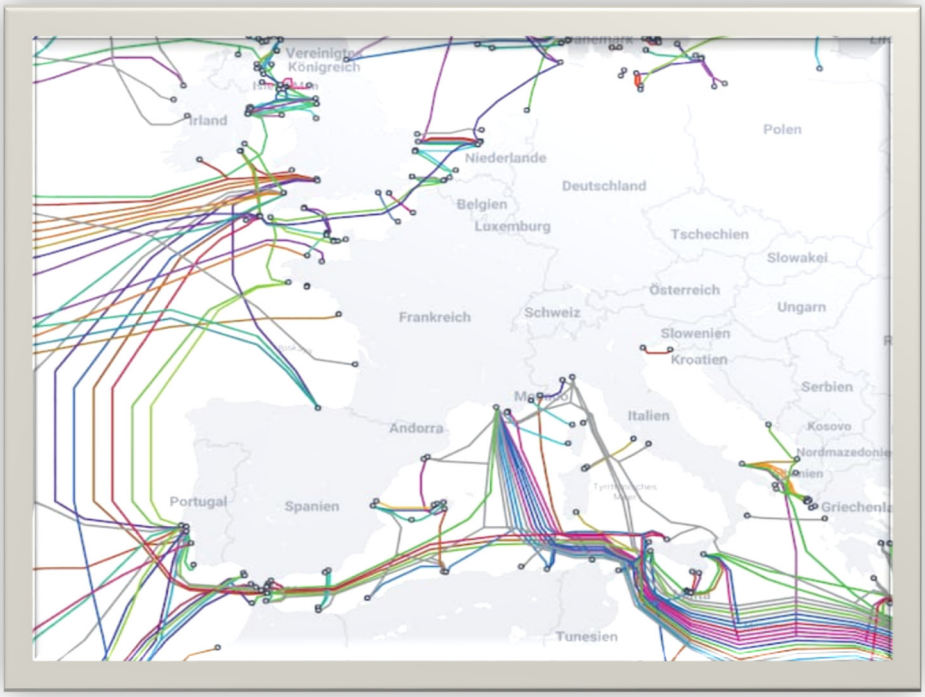
- Les conventions faites dans le cadre international ou régional restreignent les libertés des parties signataires ;
- Il existe une opposition flagrante entre les libertés publiques (telles que définies dans les Etats Occidentaux) et les mesures de surveillances ou de contrainte imposées par la cybersécurité ;
- Le nombre de matières juridiques impliquées est très grand ; Pour n'en prendre que quelques exemples :
  - Droit constitutionnel ;
  - Droit pénal ;
  - Droit financier ;
  - Libertés publiques ;
  - Droit des contrats
  - Droit de la propriété intellectuelle.

Une fois ces règles mises en place, se pose pour la majorité des citoyens, d'importantes difficultés de connaissance et d'applicabilité de la règle. « Growing regulatory demands in the US, UK, EU and other places make it almost impossible for ITO providers to be compliant with all regulatory requirements as data and services flow between regulatory perimeters, » (Al Harrack, 2021).

De la cybersécurité à la Cyber Threat Intelligence : l'emploi de la force légitime

Insistons tout d'abord sur le fait que la cyber guerre ne se contente pas de faire des dégâts matériels et financiers. Elle fait des morts. Certes, peut de victimes physiques pour l'instant, à part certainement quelques personnes non soignées dans des hôpitaux victimes de cyber attaques ; mais de très nombreuses personnes morales : « *60% des entreprises victimes de cyberattaque déposent le bilan dans les 6 mois* »[13].

Ces dégâts auxquels il faut ajouter la généralisation des attaques contre les systèmes considérés comme vitaux pour « les intérêts de la nation », entrainent ipso-facto la question de « l'emploi de la force légitime » pour riposter aux agresseurs, tout autant que celle des « frappes préventives ». A titre d'exemple, jusque là épargnés, en cette fin octobre 2022, les réseaux physiques de communication Internet sont l'objet de nombreux sabotages, notamment en France.



Source : https://www.businessinsider.com/animated-map-global-fiber-optic-internet-cables-2015-9

Figure 10. Les sources de l'Internet en Europe

[13] https://www.wedemain.fr/securite-resilience/60-des-entreprises-victimes-de-cyberattaque-deposer

Que ce soit au niveau de la sécurité nationale (voir internationale) ou à celui de la sécurité des échanges internationaux et des chaines de valeurs, force est de constater que les attaques sur les réseaux physiques deviennent critiques. Ces sabotages touchant aux intérêts vitaux de nombreux pays (Occidentaux, mais aussi Asiatiques, Africain en raison de leur importance dans l'outsourcing mondial) pourraient faire l'objet de mesures de représailles armées.

Traditionnellement cantonnée au sein des agences nationales de cybersécurité ou auprès de services spécialisés des services de police et de gendarmerie, l'emploi de la force légitime va jusqu'au développement de la cyberguerre soit asymétrique quand il s'agit de s'attaquer à des terroristes ou des mafias (Lee, 2015) ; soit classique quand il fait face aux attaques d'Etats. A cette fin, les USA ont établi « l'US Cyber Command to conduct cyber opérations » et déterminé en 2011 une « Strategy for Operating in Cyberspace » en faisant « officiellement » les 5° espace de combat (Terre, Mer, Air, Espace, Cyber).

Loin d'être une vue de l'esprit, la cyberguerre a déjà été largement théorisée (Springer, 2015 ; Green et al., 2015 ; Jajodia et al., 2015 ; Yager et al., 2015). Ceci, jusqu'à en développer une éthique (Allhoff, Henschke et al., 2016 ; Taddeo, Glorioso et al., 2017).

Dès 2008, les Nations Unies ont accrédité Le NATO Cyber Defense Center of Excellence, installé à Tallin, Estonie l'année suivante. Le droit de la cyberguerre a dès lors été précisé, notamment sous l'autorité d'un groupe d'experts mandatés par l'ONU. (Schmitt et al., 2013)

Il est probable que la guerre en Ukraine, soit l'occasion unique pour la mettre en pratique à grande échèle.

Il ressort clairement de cette seconde section, que l'Etat est l'acteur incontournable central de la mise en place, du cadrage et du pilotage de l'intelligence des risques cyber.

Conclusion

Ce trop rapide parcours dans le domaine du risque cyber, nous dresse le paysage d'un Risque d'une rare diversité, émanant d'une variété d'acteurs, pas toujours de mauvaise foi. Et encore ce cheminement ne s'est-il pas poursuivi dans le monde fantastique des organisations.

Etudiée et théorisée, l'Intelligence des Risques Cyber n'a pas encore acquis ses lettres de noblesses. Composée, de façon disparate d'une multitude de spécialités, appartenant à diverses branches de la recherché sans lien les unes avec les autres, il est vrai qu'elle est tout aussi technique que complexe. Pour s'en convaincre, il n'est qu'à synthétiser les domaines utilisés lors de cette réflexion :

Source : Auteur

Figure 11. Domaines impliqués dans l'intelligence des risques cyber

Bien trop pour un seul homme, me direz-vous. Et vous auriez raison. Au vu des défis et des enjeux de la question, il est pourtant capital de coordonner ces spécialités et de sensibiliser des populations toujours plus dépendantes des TIC à leur propre sécurité cyber. Ce d'autant le succès croissant des objets connectés (industriels ou amateurs) rajoute un niveau de risque (Bou-Harb et Neshenko, 2020).

A cette fin, nous inspirant de l'expérience tirée de l'intelligence Economique, nous proposons donc la création d'une Cyber threat intelligence, en tant que spécialité autonome.

Conflit d'intérêts

L'auteur déclare n'avoir aucun conflit d'intérêts.

Bibliographie

A., Loske. (2015). *IT security risk management in the context of cloud computing.* Darmstadt, Germany: Springer Viewer.

Ahram, T. Z., et Nicholson, D. (2018). *Advances in human factors in cybersecurity 2018.*

Springer, 2018.

Al Harrack, M. (2021). Cybesecurity risks in outsourcing strategies. *Academia Letters, Art 4161.* https:/doi.org/10.20935/AL4161.

AlDaajeh, S., Saleous, H., Barka, E., Breitinger, F. et Choo, K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computer & Security*, Vol 119-102754. https://doi.org/10.1016/j.cose.2022.102754

Allhoff, F., Henschke, A., and Strawser, B. J. (eds.). (2016). *Binary Bullets. The ethics of cyberwarefare.* Oxford University Press.

Azzeh, M., Altamimi, A. M. et Atallah Aloudat, M. (2022, 09). *Adopting the cybersécurity concept into curriculum. The potential effects on students cybersécurity knwoledge*. DOI:10.48550/arXjv.10407. Édité par Researchgate.net.

Barat-Ginies, O. (2014). Existe-t-il un droit international du cyberespace ? *Herodote*, 2014/1, 201-220.

Bartsch, M., et Frey, S. (2018). *Cybersecuritu best practices. LÖsungen zur Erhôhung cyberresilienz fur unterhement und behôrden.* Springer.

Cabriol, M. (2022). Cyber-Espionnage ; les opérations chinoises montent en puissance contre les intérêts français. *La Tribune*, 2022, 10/10.

Chmielewski, S. (22/10/22). *Le futur de l'identité et des accès : pour une gestion de l'identité numérique agile et de confiance*. Aviable at https://www.linkedin.com/pulse/le-futur-de-lidentit%25C3%25A9-et-des-acc%25C3%25A8s-b%25C3%25A2tir-une-gestion-chmielewski/?trackingId=6QcrcNBvG96p3FmXREiFgA%3D%3D

Clough, J. (2013). *Principes of cybercrime.* Cambridge University Press.

Cybermalveillance France. Aviable at https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique

Czuryk, M. (2022). Supervision and inspection in the field of cybersecurity. In: Karpiuk, M., Kostrubiec, J. (eds.). *The public dimension of cybersecurity.* Maribor, Slovenia: Lex Localis.

Dehghantanha, A., Conti, M. et Dargahi, T. (2018). *Cyber Threat Intelligence.* Springer, advances in Information Security 70.

Delville, T (30/10/2022). Aviable at https://www.wedemain.fr/securite-resilience/60-des-entreprises-victimes-de-cyberattaque-deposer

Distler, D., et Hornat, C. (2007). *Malware analysis: an introduction.* Sans Reading Room's Research Paper. Aviable at https://www.giac.org/research-papers/2103/

Groupe Pandaros (2021). *Cybers&curité, Methode de gestion de crise.* VA Editions, Col.

Guerre de l'Information.

Eriksson, J., Giacomello, G. (2007). *Internationale relations and security in the digital age.* Routledge.

Fadia, A., Nayfeh, M. et Noble, J. (2020). *Follow the leader: how governments can combat intensifying cybersecurity risks*. MacKinsley. Aviable at https://www.mckinsey.com/~/media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/Follow%20the%20leaders%20How%20governments%20can%20combat%20intensifying%20cybersecurity%20risks/Follow-the-leaders-How-governments-can-combat-intensifying-cybersecurity-risks-F.pdf

Ferens, A. (2021). Cybersecurity and cyber risk in integrated and management reports of key service operators. *Theorical Journal of Accounting*, Vol 45/2, 31-50.

Gigerenzer, G. (2004). Dread risk, september 11, and fatal traffic accidents. *Psychological Science,* 15, No 4, 286-287.

Green, J. A. (2015). *Cyber warfare. A multidisciplinary analysis.* Routledge.

Helbing, D. (2013). Globally networked risks and how to respond. *Nature*, Issue 497, 51-59. Aviable at: https://doi.org/10.1038/nature12047

Hepple, B. (2005). *Labour laws and global trade.* Hart Publishing.

Jajodia, S., Shakarian, P., Subrahmanian, V. S., Swarup, V., Wang, C. (2015). *Cyber warfare. Building the scientific fundation.* Springer.

Jajodia, S., Kant, S. (2014). *Secure cloud computing.* Springer.

Kaczmarek, K. (2022). Digital competencies of the general public and the state's vulnerabilities to cyberspace treats. In: Karpiuk, M., Kostrubiec, J. (eds.). *The public dimension of cybersecurity.* Maribor, Slovenia: Lex Localis.

Karpiuk, M., et Kostrubiec, J. (2022). *The public dimension of cybersecurity.* Maribor, Slovenia: Lex Localis. Aviable at https://www.researchgate.net/publication/362656795.

Kendall, K., et McMillan, C. (2007). *Practical malware analysis*. Black Hat Conference. USA.

Kittichaisaree, K. (2017). *Public International law of cyberspace.* Springer.

Kizza, J. M. (2014). *Network Security ans Cyber Ethics.* 4 Ed. McFarland & Cie.

Kshetri, N. (2010). *The global cybercrime industry.* Springer.

Lee, N. (2015). *Counterterrorism and cybersecurity. Total information awarneness.* 2 Ed. Springer.

Loske, A. (2015). *IT' Security Risk Management in the context of cloud computing.* Springer.

Marczcyk, M. (2018). Cyberprzestrzen jako nowy wymiar aktywnosci czlowieka - Analiza Pojectciowa obszaru. *Przeglad Teleinformatyczny*, 1-2, 59-72.

Martre, H. (1994). *Rapport sur l'Intelligence Economique.* La Documentation Française.

Mhalla, A. (2022). Il est temps de nous préparer aux cyberguerres. *Le Figaro*, 14. 10. 2022.

Moallem, A. (2018). Cybersécurity awarness among college students. In: Ahram, T. Z. et Nicholson, D. (eds.). *Advances in human factors in cybersecurity.* Springer.

Nicholson, D. (ed.). (2016). *Advances in Human Factors in cybersecurity, 2016.* Springer.

Nicholson, D. (ed.). (2017). *Advances in human factors in cybersecurity, 2017.* Springer.

Numérama, 2/11/2022. Aviable at https://www.numerama.com/cyberguerre/1167442-les-hackers-criminels-russes-peuvent-etre-tranquilles-moscou-ne-les-arretera-jamais.html.

Obaidat, M. S., Traore, I., Woungang, I. et al. (2019). *Biometric based physical and cybersecurity systems.* Springer.

Pieczywok, A. (2022). Cybersecurity and school-age young people. Challenges and threats. In: Karpiuk, M., Kostrubiec, J. (eds.). *The public dimension of cybersecurity.* Maribor, Slovenia: Lex Localis.

Pilzo, W.(2022). Management in cyberspace : from firewall to zero trust. In: Karpiuk, M., Kostrubiec, J. (eds.). *The public dimension of cybersecurity.* Maribor, Slovenia: Lex Localis.

Richards, J. (2017). *Cyber-War. The anatomy of the global security threat.* Palgrace Macmillan.

Rougé, J. F. (2020). *La petite entreprise: un sanctuaire face à la cyberguerre !* Comment en finir avec ce mythe dangereux? Aviable at: https://www.researchgate.net/publication/340600332_La_petite_entreprise_un_sanctuaire_face_a_la_cyberguerre_Comment_en_finir_avec_ce_mythe_dangereux

Schmitt, M. N. (2013). *Tallinn Manual on the international law applicable to cyber warefaire.* Cambridge University Press.

Shackleford, D. (2015). *Who is Using cyberthreat intelligence and how?* Aviable at https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767.

Sikos, L. F. (ed.). (2019). *AI in cybersecutity.* Springer.

Skopick, F. (ed.). (2018). *Collaborative cyber Threat Intelligence. Detecting and responding to advanced cyber attacks at the national level.* CRC Press, Taylor & Francis Group.

Springer, P. J. (2015). *Cyber warfare. A reference handbook.* ABC-CLIO.

StealthLabs. (2020). *Cybersecurity Threats and attacks: all you need to know.* Aviable at https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/

Taddeo, M., Glorioso, L. (eds.). (2017). *Ethics and policies for cyberopérations. A NATO cooperative Cyber Defence Center of Excellence.* Springer.

Taliharn, A.-M. *En quête de la cyberpaix : gérer la cyberguerre par la coopération internationale.* Aviable at https://www.un.org/fr/chronicle/article/en-quete-de-la-cyberpaixgerer-la-cyberguerre-par-la-cooperation-internationale

Tyrawa, D. (2022). The axiological and legal aspects of multi-faceted nature of cybersécutity. In: Karpiuk, M., Kostrubiec, J. (eds.). *The public dimension of cybersecurity.* Maribor, Slovenia: Lex Localis.

Voig, P., von dem Bussche, A. (2017). *The EU General Data Protection Regulation. A practical guide.* Springer.

Willcocks, L. P., et Lacity, M. (2012). *The new IT outscourcing landscape. From innocation to cloud services.* Palgrave Macmillan.

Yager, R. R., Reformat, M. Z., Alajlan, N. et al. (2015). *Intelligent methods for cyber warfare.* Springer.

Annexe 1

Modèle de Procedures de sécurité annexé à un contrat de travail dans une firme du secteur IT

COMPUTER SECURITY PROCEDURES

1. APPLICABILITY

1.1. This policy applies to all employees of the Company.

1.2. If there are specific policies with Company's clients in case the employee works in client's environment, then apply both of the policies – the current Company policy and the Client's computer policy. In the event of any discrepancies the current Company policy shall prevail.

1.3. In order to log on to the Company network, you are asked to type a login name and a password. This password is the single most important aspect of security protection on our network, and you will be asked by the system to change it every 60 days.

Do not disclose your password to anyone else; if you do disclose your password change it again as soon as possible.

Do not make your password obvious, such as your name or date of birth.

Do not write your password down.

Do not let anyone else use your password. If you are going on holiday you should not disclose your password as IT can arrange for your manager to have access to your files and email.

Do not leave your system logged on if you are out of the office for any length of time.

1.4. Communication of Trade Secrets

Unless expressly authorized by the Company's CEO, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the company is strictly prohibited.

1.5. Backups

Remember always save your work as often as you can afford to lose it!!

Backups are automatically completed if you use a network computer and save your files on a network shared drives. However, if you are working on a standalone or portable, then taking back-ups is your own responsibility. No one can help you if you haven't taken a backup and an unfortunate occurrence, such as failure of your hard

disk takes place. If you use a laptop and regularly connect to the network, you should copy all files in your work directory onto your personal drive of the network. If you need help with this speak to the IT Servicedesk.

1.6. Virus infection

Computer viruses are a class of program written to cause some form of intentional damage to computer systems or networks. They are a real and significant threat to the company. We have a virus protection system in place. This will check any floppy disks /CD's and flash devices automatically when you first try to read them. It also checks the hard disks of Network machines every time you log into the Network. The File Server is fully checked for viruses on a nightly basis. We also check all incoming (and outgoing) emails.

If you do get a virus alert from the system, **DO NOT IGNORE IT**. Please immediately contact a member of the IT Department before attempting to use the resources again.

1.7. Games / Personal programs

Your PC is configured and specified for work purposes. Games and personal programs consume resources such as computer memory, and may have unexpected side effects on the configuration of your machine. IT support staff will not support any unauthorized software. Therefore, NO GAMES, PERSONAL PROGRAMS, SCREEN SAVERS OR BACKGROUNDS are to be loaded onto the Company's computers or networks.

If you have particular software package that will help your job function, and the Company has not provided the software, discuss the issue with the IT Manager. If agreed, we will organize the loading of the software. A form must be signed to declare that you are properly licensed for the software in question, and that you have not violated your license agreement by having loaded the software elsewhere.

1.8. Reporting the theft or loss of computer equipment

Users are responsible for the computer equipment issued to them and will be asked to sign a document to confirm receipt, accepting responsibility for the item(s).

If **ANY** equipment is lost or stolen from the office, site, car, home or in transit, you **MUST** report it immediately to IT Department and your manager.

If the equipment has been stolen it must be reported to the Police immediately and you **MUST** obtain a crime report and report number.

1.9. Allocation of computer equipment

It is the responsibility of the IT Department to allocate computer equipment to users, any transfer of computer equipment between users and locations within the office or between offices or office and site must be with the full knowledge and authorization of the IT Manager.

2. THE COMPUTER POLICY ON EMAIL

The e-mail system is provided to employees at company expense to assist employees in carrying out company business. The use of the email system is solely to conduct business. It is not intended for personal business. The company treats all information transmitted through or stored in its computer system, including email messages as company business information. They are not the private property of any employee.

The company has the capability to access, review, copy, modify, add, and delete any information in its computer system as it sees appropriate. Accordingly, employees should not use the system for any information they wish to keep private.

Do not treat email as a casual form of communication. It requires the same amount of thought you would put into a letter.

Comply with email etiquette – typing emails in capital letters is the equivalent of SHOUTING!

An email communication is as legally binding as a letter. Improper statements can give rise to personal or Company liability.

Do not commit to any commercial or contractual terms in an email that you would not put in a letter.

Do not send information or documents, however innocently, that may be offensive to a recipient.

Do not send emails that are in any way illegal, defamatory, racially or sexually objectionable, pornographic or inconsistent with our standing as an equal opportunities employer. You must discourage any third party from forwarding emails that fall into any of the preceding categories. • Do not put anything in an email that you would not wish to say to an organization or individual personally.

Passing off an email as coming from someone else or in any way secretly tampering with someone else's text – even if meant in good humor – is strictly forbidden.

Do not open colleagues' emails unless authorized by them to do so.

External email can be intercepted by and read by a third party. Confidential information, e.g., bank account details, should never be sent in an external email.

3. THE COMPUTER POLICY ON INTERNET

3.1. Availability of access

The use of the Company's connection to the Internet is intended for business-related communications. No one other than the Company's employees may use this connection to send or receive messages or download information.

The Company, at its sole discretion, may determine whether an employee has unlimited, limited or no access to the Internet through its IT systems and may from time to time authorize senior managers to make decisions concerning an individual employees' access.

To enhance Network security and avoid the spread of computer viruses, accessing the Internet directly, by modem, is strictly prohibited.

3.2. Personal use

Personal use of the Internet is permitted where such use is:

incidental to employment and occasional in nature; and

not detrimental to the company in any way; and

not in breach of any term and condition of employment; and

not such as to place the employee or the company in breach of statutory or other legal obligations.

3.3. Monitoring

The Company reserves the right to monitor all use of the Internet through its IT systems. Any excessive use of the Internet resulting in inappropriate costs may be considered an abuse and employees may be subject to disciplinary action including, in appropriate circumstances, dismissal.

The Company has the right to review all software held on employees' PC's to ensure they are used only for business purposes.

3.4. Disclosure of Internet information

Disclosure of information downloaded from the Internet should be limited to employees who have a reasonable need for access to the information.

Communications over the Company's connection are not private and employees should have no expectation of privacy. Messages may be lost in transit, read or potentially altered in transit.

3.5. Specific rules

The Company specifically prohibits the use of the Company's IT systems to:

Make official commitments through the Internet on behalf of the company or group unless prior arrangements have been approved by a Director

Download or disclose information available from the Internet, including but not limited to information which is sexually, violently, racially or religiously graphic or inflammatory in nature, pornographic, frivolous or trivial, blasphemous, scandalous or otherwise abusive in any way to members of staff, the company, its clients, supplier's

and competitors;

Make personal gains (at the expense of the company or the group) or for conducting a personal business

Gambling and the sending of chain letters

Break the law

Bring discredit to the Company, intentionally or inadvertently (by obtaining or circulating any information obtained from the Internet)

Employees are discouraged from accessing the Internet at any time during working hours other than for work purposes

3.6. Copyright issues

Materials on web sites or other external systems or email messages and attachments which employees receive may contain intellectual property belonging to others (including copyright, trade secrets or trademarked information). Employees may not use the company's connection in a way which infringes upon any party's copyright or related rights. Violations of copyright (or other similar rights) may subject them and the company to civil and or criminal penalties.

As a general rule, employees may not forward, distribute or incorporate into other work, material received from a web site or other external system. Very limited "fair use" may be permitted in certain circumstances. Browsing or viewing material on the PC is, however, generally permissible.

4. KEY PRINCIPLES OF THE COMPUTER POLICY General

Do not disclose your password.

Do not leave your system switched on overnight.

Lock laptops away at night.

Save/backup your work regularly.

Do not ignore computer virus alerts

Do not load any games or personal programs.

Report the theft or loss of computer equipment immediately.

E-mail

Do not treat email as a casual form of communication.

Do not send emails that are inconsistent with our standing as an Equal Opportunities employer.

Do not open colleagues' emails unless authorized by them to do so.

Communicate via email as you would in a face-to face discussion or in a letter.

Internet

Access to the Company's Internet connection is intended for business-related communications. • Communications over the Company's Internet connection are not private – the Company will monitor all Internet activity.

The Internet is not to be accessed for any material which is pornographic and/or inconsistent with our standing as an Equal Opportunities employer.

You are encouraged to use the Internet to obtain business related information and use the Internet to substitute more expensive traditional research methods.

I accept that the Company may, on occasions, listen in on my business telephone calls. I also accept that e-mails are routinely intercepted and emails which may not be considered work related can be read.

I confirm that I have read and understood the Company Computer Policy. I agree that the obligations contained within this policy now form part of and shall be incorporated into my Contract of Employment. I understand that any infringement of this policy may result in disciplinary action including, in appropriate circumstances, dismissal for gross misconduct and may also expose me to personal liability and civil or criminal penalties.

Signed:……..

Name:……..

Date:……

Cybersecurity and new technologies for regulated and innovative economic development

Jean-François Rougé, PhD, est Professeur des universités françaises d'économie, de droit et de gestion, consultant, jfrouge@yahoo.ca

Jean-François Rougé, PhD, is Professor at French universities of economics, law and management, consultant, jfrouge@yahoo.ca

CYBER THREAT INTELLIGENCE. HOW TO PUT IN PLACE A GLOBAL APPROACH TO FIGHT THE RISE IN IT RISKS?

Abstract: Cyberspace became the battlefield of new kinds of wars that have already changed the face of the world. To challenge those threats, we have to create a Cyber Threat Intelligence. It should be global, multi-disciplinary and must include different kind of actors with quite diverse competencies, powers and action capacities. Confronted to this huge task, this paper asks a question: How to deal globally with always more critical cyber threats? To answer this question, this article is based on research conducted in economic intelligence. It focuses practically on two axes of action: limiting human risk and specifying the public action necessary to fight cyber-attacks.

Keywords: Cybersecurity; Cyber Threat Intelligence; Cyberwarefaire; Business intelligence; Geostrategy; Computer Law

JEL codes: B59

How to cite this article:

Rougé, J.-F. (2023). Cyber threat intelligence. Comment mettre en place une approche globale pour lutter contre la montée des risques informatiques ? (Cyber Threat Intelligence. How to Put in Place a Global Approach to Fight the Rise in It Risks?). *Economic Thought Journal*, 68 (6), 642-673 (*in French*).
https://doi.org/10.56497/etj2368603