Insee
Mesurer pour comprendre
Direction générale

CONCOURS INTERNE DE CONTRÔLEUR DE L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES

ANNÉE 2019

ÉPREUVE DE RÉSUMÉ DE TEXTE
ET DE RÉPONSES À DES QUESTIONS SUR CE TEXTE

Décembre 2018

(Durée : 3 heures, coefficient:4)

Le sujet comporte 6 pages (y compris celle-ci)

CINRES191

I : Résumer en 350 mots (une marge de plus ou moins 10 % est admise) l'article suivant de Nima Sanandaji (Traduit par Bérengère Viennot) paru dans la version française du magazine en ligne Slate en septembre 2018.

Rappel : le résumé de texte est une miniaturisation qui respecte la structure du texte initial.

Le candidat indiquera obligatoirement, à la fin du résumé, le nombre de mots utilisés. Il est rappelé que les articles élidés (l'ou d') comptent pour un mot.

Le non-respect des consignes sera sanctionné par le jury.

II : Répondre aux **deux questions** suivantes :

Question 1
Quelles sont les caractéristiques de la politique de solidarité suédoise de 1932 à 1976 ?
(Répondre en quelques lignes)

Question 2
Pensez-vous que nous vivons dans une société solidaire ?
(Répondre en deux pages environ)

NOTA :

1° — Dans cette épreuve, il sera tenu compte de la longueur du résumé, de la clarté de la rédaction, de l'orthographe et de la présentation.

2° — Les réponses aux questions devront être structurées et rédigées.

3° — Le barème de notation sera le suivant :

Résumé: 10 points

Question 1 : 2 points

Question 2 : 8 points

La Suède ou le deuil d'un modèle social

Nima Sanandaji — Traduit par Bérengère Viennot — 11 septembre 2018 à 8h26 — mis à jour le 11 septembre 2018 à 8h26.

Il est assez rare que des idéaux politiques finissent au rayon nostalgie. Ceux qui connaissent le succès vivent dans la rue et la vie quotidienne, ceux qui périssent le font dans l'obscurité.

En ce moment, le Nordiska Museet, le grand musée d'anthropologie de Stockholm, abrite une exposition dédiée à un mot, un seul, qui jusqu'à une période récente insufflait un souffle vital à la Suède et qui aujourd'hui hante sa politique nationale par son absence.

Ce mot, c'est *folkhemmet*, et l'idéal qu'il incarne –tout comme le vide laissé par son absence– contribue à expliquer la résurgence du populisme réactionnaire secouant l'ordre politique du pays et du continent tout entier. Il se trouve que *folkhemmet* n'a pas d'équivalent en anglais [et en français non plus, ndt]. La traduction littérale « la maison des personnes » est un peu poussive, mais elle en capture le concept principal: celui du foyer.

L'exposition du Nordiska Museet rend très clairement cette idée. Elle montre la reconstitution complète d'un appartement de la fin des années 1940, construit par le gouvernement pour un travailleur qualifié et sa famille. Aux yeux des visiteurs et visiteuses contemporaines, cet appartement peut sembler exigu, mais loin d'être miteux –les placards de cuisine pastel passeraient même facilement pour du rétro-chic.

À l'époque où il a été réalisé, ce foyer représentait une prospérité quasiment inimaginable pour la famille qui y vivait: il avait l'eau courante, chaude et froide, un accès à une buanderie commune, des espaces de rangement, des fondations et des murs extérieurs en béton bien solide. Mais par-dessus tout, en termes d'idéal de *folkhemmet*, ce foyer n'était pas une récompense, quelque chose que la famille avait dû mériter en réalisant une action extraordinaire. Cet appartement, cette famille le méritait par sa simple appartenance à la communauté suédoise.

L'histoire avait commencé ailleurs. Le mot vient de l'allemand *Volksgemeinschaft*, ou « communauté du peuple », que plus personne n'utilise parce qu'il était devenu un slogan nazi. L'expert en sciences politiques de droite Rudolf Kjellén l'introduisit au début du XX^{e} siècle en Suède, où le leader social-démocrate Per Albin Hansson s'en empara et le transforma en slogan politique et en programme de gauche.

Dans un discours en 1928, Hansson déclara: *« Dans un bon foyer, il n'y a* [...] *ni préférés, ni beaux-enfants. Personne n'est moins bien traité que les autres. Personne ne tente d'obtenir des avantages aux dépens d'un autre; les forts n'oppriment pas les faibles.* [...] *Appliqué à la société dans son ensemble, ceci demanderait que nous démolissions toutes les barrières sociales et économiques qui répartissent aujourd'hui les citoyens en privilégiés et en laissés-pour-compte, en ceux qui décident et ceux qui en dépendent, en ceux qui pillent et en ceux qui sont pillés. »*

Il y a toujours eu quelque chose d'insuffisant dans la traduction officielle en anglais de ce que proposa le mouvement des sociaux-démocrates: l'expression *« Welfare State »*, ou État-providence, ne capte ni la nuance émotionnelle, ni celle culturelle du terme *folkhemmet*. Elle donne l'impression d'une vaste administration impersonnelle qui réglementerait la vie des gens, alors que cette vision envisageait plutôt une administration très personnelle –une extension de la politique de la solidarité imposée déjà inscrite dans la culture suédoise.

Pendant la plus grande partie de son histoire, la Suède a été une société plutôt autoritaire. Un véritable réseau de formalités et d'obligations, codifiées seulement en partie par le droit, assurait que chacun ou chacune restait à sa place et en pleine conscience de sa position sociale relative. Les libertés individuelles étaient strictement limitées.

De 1919 à 1955, l'alcool fit l'objet d'un rationnement obligatoire, avec des quantités qui variaient en fonction de l'âge, du statut social et du sexe: les hommes avaient droit à trois litres d'alcool par mois; les femmes mariées n'avaient droit à rien, mais les femmes célibataires pouvaient, lorsqu'elles avaient de la chance, obtenir un demi-litre d'alcool tous les trois mois –cependant, seule une femme sur dix disposait d'un carnet de rationnement. Et jusqu'en 1951, il était techniquement illégal d'être athée en Suède –mais on pouvait choisir parmi un éventail de onze religions officielles.

Ce qu'ont fait les sociaux-démocrates en introduisant le *folkhemmet* au début du XX^{e} siècle, c'est préserver le strict sentiment de l'ordre communautaire suédois –avec cette même impression que tout le monde, plutôt qu'un seul Big Brother, vous surveillait tout le temps– tout en changeant le dogme sous-jacent et en substituant à l'autorité de Dieu et à l'espoir du salut l'autorité de la science et l'espoir du progrès.

Le résultat fut un sentiment de solidarité nationale d'une nouvelle sorte, dont les Suédois et Suédoises ont dû accepter les termes et les conditions sans poser de question ni protester. Et c'est ce que furent ravies de faire la plupart d'entre elles et eux, en votant pour maintenir les sociaux-démocrates au pouvoir, à partir de 1932, pendant quarante-quatre années consécutives.

Pendant cette période, le gouvernement suédois mit au point un système de santé universel, d'éducation supérieure gratuite et de logement social. Mais son expression la plus claire de l'idéal du *folkhemmet* fut la création du système de garde d'enfants public et accessible à tous. Cette politique n'avait pas pour visée un bénéfice économique; elle avait pour ambition de transformer le rôle de la femme dans la société.

On en doit l'idée aux personnalités sociaux-démocrates Gunnar et Alva Myrdal, qui dans les années 1930 avancèrent que des politiques familiales égalitaires encourageraient à la fois les femmes à avoir plusieurs enfants et à rejoindre les rangs de la population active. L'idéal des Myrdal était que non seulement la garde des enfants et l'éducation mais aussi les naissances se distribuent de façon égale dans toute la société; leur espoir était que les familles de toutes les classes aient en moyenne trois enfants. Le but n'était pas que les aménagements prévus par le gouvernement en matière de grossesse et de garde d'enfants soient bons pour les femmes, mais qu'ils le soient pour la société dans son ensemble.

Ces projets furent dûment traduits en politiques concrètes par les gouvernements sociaux-démocrates consécutifs. En 1975, les autorités locales étaient obligées de scolariser tous les enfants de 6 ans. En pratique, cela s'appliquait aussi aux enfants bien plus petits. Avant le crash économique du début des années 1990, on en était venu en Suède à considérer comme presque immoral pour une femme de rester à la maison pour s'occuper de ses enfants, tendance qui disparut lorsque le taux de chômage commença à grimper.

L'État se consacra ensuite à s'assurer que les hommes prenaient leur part du soin aux enfants et ne privilégiaient pas le travail, avec un mélange de pression légale et sociale pour garantir que le congé parental payé était réparti de façon plus égale. Ces politiques et les normes culturelles qui leur sont associées ont peu, voire pas d'équivalent hors de Scandinavie.

Peut-être le meilleur moyen de capter le sens du *folkhemmet* passerait-il par le biais d'une traduction très libre, quelque chose comme « famille nationale ». Le principe de la famille, ce n'est pas que ses membres soient heureux, ni même qu'ils s'aiment –comme le montrent d'ailleurs très bien les films du réalisateur suédois Ingmar Bergman, mais qu'ils soient tous coincés les uns avec les autres. À long terme, ils vont être obligés de s'entendre, ou en tout cas de s'adapter à leur haine mutuelle. Et cette adaptation prend le pas sur tout le reste.

Dans ce sens, la cohésion des familles est assurée par des engagements innés, pas par des contrats volontairement souscrits. Ce sont des institutions profondément oppressives. Personne ne demande à naître dans une famille et pourtant, une fois que vous en devenez membre, les autres doivent vous accepter. Ce que la Suède a réussi, c'est à transformer mine de rien le sentiment que les Suédois et Suédoises s'accordaient bien en un sens d'obligation mutuelle.

Ce sentiment d'appartenance n'a en aucun cas totalement disparu de Suède. Les personnalités politiques de droite ont gardé un sens du devoir envers les pauvres et les marginaux qu'on aurait peine à trouver dans la politique britannique et américaine.

Mais cette solidarité s'est diluée au cours des dernières années –un état de choses que beaucoup mettent sur le compte de l'immigration, tout particulièrement venue des pays musulmans. Historiquement, cependant, la situation est plus compliquée que cela.

À partir des années 1950 et 1960, la Suède a commencé à accepter des travailleurs et travailleuses immigrées, principalement en provenance de Finlande, mais aussi des Balkans. Cela ne s'est pas traduit par des problèmes sociaux majeurs, peut-être parce que le processus s'était fait en accord avec les puissants syndicats du pays, qui ne considéraient pas le phénomène comme une menace pour les emplois de leurs membres.

L'immigration politique commença dans les années 1970, avec des réfugiées et réfugiés d'Amérique latine venus du Chili, où venait de se dérouler le coup d'État d'Augusto Pinochet, et avec d'autres personnes de gauche en exil. Elles furent suivies par des Kurdes ou des Assyriennes et Assyriens fuyant la guerre Iran-Irak. Puis arrivèrent les réfugiées et réfugiés des guerres de Yougoslavie, du Liban, de Somalie et de la Corne de l'Afrique puis, enfin, de Syrie.

De nombreux Suédois et Suédoises, en envisageant les membres de ces groupes, voient des gens qui déparent la famille nationale traditionnelle, notamment parce qu'elles et ils imaginent que les personnes immigrées ont des loyautés qui priment sur ses valeurs. Il est évidemment impossible d'être certain que ce soit vrai. Mais la seule possibilité d'une dilution de la loyauté nationale au sein d'une partie de la population pourrait avoir affaibli le lien inconditionnel que la population suédoise voyait auparavant entre patriotisme et socialisme et qui était implicitement contenu dans le concept de *folkhemmet* depuis le début.

De nombreux autres facteurs ont œuvré dans la même direction. Bien avant que l'immigration de masse en Suède ne devienne un phénomène, puis un problème, l'ancien modèle s'était déjà brisé de l'intérieur.

D'abord, dans les années 1970, on a assisté à l'effondrement de la culture de la déférence envers l'autorité –un affaissement causé par les sociaux-démocrates eux-mêmes. Si la première génération au pouvoir avait largement libéré le pays de la peur de la pauvreté, la génération suivante, conduite par le Premier ministre Olof Palme, sembla parfois vouloir libérer en une seule fois le peuple de toutes les chaînes inégalitaires qu'il restait. Les sociaux-démocrates n'avaient pas prévu que ce tournant allait saper l'autorité de leurs propres institution politiques.

Vint ensuite la crise économique des années 1980 et 1990. Le *folkhemmet* avait été conçu dans l'austérité des années 1930 et 1940, mais il avait atteint sa maturité lors de la grande vague de prospérité d'après-guerre, lorsque les fonds publics semblaient intarissables. En 1975, la garantie de sécurité promise par l'État au public commença à paraître inabordable. Le pays se détourna de la planification centrale pour s'orienter vers une forme de capitalisme bien plus décentralisée et moins réglementée.

Ce changement alimenta une transformation culturelle. L'introduction de la télévision commerciale exposa les Suédois et Suédoises à des hiérarchies de capital social et économique aussi nouvelles que séduisantes. Ces hiérarchies étaient plus alléchantes que l'unité guindée du *folkhemmet* précisément parce qu'elles étaient moins égalitaires.

Dans le même temps se produisit un énorme phénomène d'exode rural, qui détendit les liens et les réseaux traditionnels. De façon plus subtile, cela réduisit les opportunités de chacun et chacune de se sentir, et d'être, importante dans sa propre sphère ou dans sa communauté. Lorsqu'il y a beaucoup de petits étangs, chacun aura son gros poisson ; quand il n'y a qu'un seul lac énorme, bien moins de poissons peuvent être considérés comme vraiment gros. Il ne suffisait plus d'être quelqu'un d'important dans une ville de province ou une usine locale –et d'ailleurs, ces dernières disparurent aussi, lors de la grande désindustrialisation des années 1980 et 1990.

Presque tous ces changements prirent l'apparence de mesures progressistes à l'époque, et la plupart étaient absolument inévitables. Mais tous contribuèrent plus ou moins à réduire ce sentiment d'appartenance et à remplacer les engagements par des contrats et l'immobilité de fait par une liberté périlleuse.

Les impôts furent réduits, les congés maladie et les allocations chômage baissèrent; la présence de l'État s'amoindrit dans le cadre d'une vague de privatisations, qui inclut notamment celle de la poste et des chemins de fer –aujourd'hui objets de honte et de colère nationale pour leur incapacité chronique à fournir des services corrects.

La dernière fois que je suis allé à Stockholm, en mai, un éminent journaliste du journal Dagens Nyheter –quelqu'un qui évolue au sein même de l'élite progressiste– m'a expliqué rageusement à quel point ces deux échecs lui donnaient l'impression que son pays était perdu et s'était éloigné de ses valeurs. Celles-ci avaient toujours inclus la compétence, la fiabilité et des infrastructures sociales en état de fonctionner. Maintenant, plus rien n'est à l'heure, même pas les trains. Le sentiment que le pays n'est plus lui-même s'étend bien au-delà d'un simple malaise autour de l'immigration.

Cette perte de la sensation des Suédois et Suédoises qu'elles et ils ont un foyer, et vivent dans un endroit où l'on doit vous accepter même si vous ne le méritez pas, hante leur politique actuelle –et plus largement toute la politique européenne. C'est l'un des grands facteurs de xénophobie, parce qu'elle met l'accent sur des questions qui ne se posaient jamais jadis: qui mérite une place dans la famille, et pourquoi ?

Le fait de pleurer la perte du *folkhemmet* revient à reconnaître la fin de tout sens d'obligation mutuelle. Pas facile d'imaginer quelles politiques, quelles politiciennes ou politiciens seraient capables de redonner vie à un tel sentiment aujourd'hui.

En attendant, de nombreux Suédois et Suédoises choisissent de compenser la perte de leurs propres idéaux de gauche en glissant un bulletin de l'extrême-droite dans l'urne. Contrairement à la plus grande partie de l'*establishment* suédois, les populistes, au moins, reconnaissent que ces idéaux ont été brisés.

Insee
Mesurer pour comprendre
Direction générale

CONCOURS INTERNE DE CONTRÔLEUR DE L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES

ANNÉE 2019

ÉPREUVE DE STATISTIQUES

Le présent document comprend 5 exercices indépendants.

Le candidat devra être attentif au contenu des questions afin d'y répondre de façon précise.

- **L'usage de la calculatrice est autorisé.**
- **Il sera tenu compte dans la notation tant de la présentation des tableaux et graphiques demandés que de la pertinence et de la clarté des commentaires.**
- **Sauf consignes particulières, les résultats seront donnés avec une décimale.**

Décembre 2018
(Durée : 3 heures, coefficient :4)
Le sujet comporte 6 pages

Exercice 1
(5,5 points)

À l'aide de la figure 1, répondre aux questions suivantes :

1- Quelle est la population des Hauts-de-France au 1er janvier 2016 ?

2- Quel département a connu la plus forte évolution relative de sa population entre 2015 et 2016 ?

3- À partir des données 2015, comment peut-on retrouver la population 2016 ? Dans ces départements, quel est le moteur de la croissance démographique (lorsqu'elle a lieu) ?

4- Quel est, en 2015 et pour chaque département, le nombre de naissances et de décès ?

5- Rédiger une note de lecture du taux de natalité en 2015 de l'Aisne.
Calculer le taux de natalité régional.

6- Rédiger un commentaire global de la figure 1 (une dizaine de lignes maximum).

Figure 1

Bilan démographique dans les cinq départements des Hauts-de-France

	Aisne	Nord	Oise	Pas-de-Calais	Somme
Population au 1er janvier 2016	537 865	2 617 319	826 773	1 477 429	570 923
Population au 1er janvier 2015	539 058	2 611 596	823 020	1 475 944	571 542
Solde naturel en 2015	+ 539	+ 11 938	+ 4 034	+ 3 113	+ 568
Solde migratoire apparent en 2015	- 1 732	- 6 215	- 281	- 1 628	- 1 187
Taux de natalité en 2015 (‰)	11,6	13,3	12,9	12,0	11,0

Source : Insee - État civil, Estimations localisées de population.
Note : Le solde naturel est la différence entre le nombre de naissances et le nombre de décès enregistrés au cours de l'année.
Le solde migratoire est la différence entre le nombre de personnes qui sont entrées sur le territoire et le nombre de personnes qui en sont sorties au cours de l'année.
Le taux de natalité est le rapport du nombre de naissances de l'année à la population totale de l'année.

Exercice 2
(6 points)

À l'aide des figures 2 et 3, répondre aux questions suivantes :

1- De quelle source sont issues les données ? S'agit-il d'un fichier administratif ou d'une enquête ?

2- Combien de femmes vivaient seules en France en 2008 ?

3- a. Calculer, pour chaque sexe, la répartition par âge des personnes vivant seules en 2014. Présenter les résultats sous forme de tableau et proposer une note de lecture.
b. Commenter.

4- a. Calculer pour chaque tranche d'âge la part des femmes ainsi que celle des hommes vivant seuls en 2014. Présenter les résultats sous forme de tableau et proposer une note de lecture.
b. Représenter les résultats sous forme de graphique et commenter.

5- En supposant que la dynamique entre 2014 et 2015 soit la même que celle entre 2008 et 2014, estimer, en millions avec deux décimales, le nombre de personnes âgées de 80 ans ou plus vivant seules en 2015.

Rappel : le taux d'évolution annuel moyen entre l'année x_1 et l'année x_2, séparées par n années est :

$$\left(\sqrt[n]{\frac{V_{x2}}{V_{x1}}} - 1\right)*100$$

Figure 2
Nombre de personnes habitant seules (en milliers)

Groupe d'âges	1999			2008			2014		
	Hommes	**Femmes**	**Total**	**Hommes**	**Femmes**	**Total**	**Hommes**	**Femmes**	**Total**
0-19 ans	64	80	144	75	96	172	94	114	208
20-29 ans	672	635	1 307	725	670	1 396	738	684	1 422
30-39 ans	608	372	980	688	408	1 097	687	403	1 089
40-49 ans	501	349	850	654	400	1 054	733	423	1 155
50-59 ans	384	476	860	621	746	1 367	745	784	1 528
60-69 ans	334	713	1 047	420	797	1 217	620	1 071	1 691
70-79 ans	298	1 100	1 398	336	1 086	1 423	361	987	1 347
80 ans ou plus	163	745	908	247	1 110	1 357	320	1 299	1 619
Total	**3 025**	**4 470**	**7 495**	**3 768**	**5 314**	**9 082**	**4 296**	**5 764**	**10 060**

Champ : France, population totale, âge en années révolues.
Sources : Insee, recensements de la population de 1999, 2008 et 2014.

Figure 3
Population totale (en milliers)

Groupe d'âges	1999			2008			2014		
	Hommes	**Femmes**	**Total**	**Hommes**	**Femmes**	**Total**	**Hommes**	**Femmes**	**Total**
0-19 ans	7 981	7 623	15 604	8 134	7 764	15 898	8 266	7 886	16 152
20-29 ans	4 107	4 079	8 186	3 968	3 999	7 968	3 893	3 916	7 809
30-39 ans	4 401	4 478	8 879	4 263	4 331	8 594	4 054	4 170	8 224
40-49 ans	4 290	4 374	8 664	4 417	4 558	8 975	4 464	4 567	9 031
50-59 ans	3 298	3 329	6 627	4 158	4 372	8 530	4 197	4 425	8 621
60-69 ans	2 601	2 952	5 553	2 875	3 113	5 987	3 625	3 957	7 582
70-79 ans	1 883	2 629	4 512	2 065	2 738	4 803	2 079	2 582	4 661
80 ans ou plus	667	1 489	2 155	1 066	2 116	3 182	1 327	2 499	3 827
Total	**29 227**	**30 953**	**60 180**	**30 945**	**32 991**	**63 937**	**31 906**	**34 001**	**65 907**

Champ : France, population totale, âge en années révolues.
Sources : Insee, recensements de la population de 1999, 2008 et 2014.

Exercice 3
(5,5 points)

À l'aide des figures 4 et 5, répondre aux questions suivantes :

1- Citer le (ou les) caractère(s) étudiés ainsi que les modalités associées.

2- Calculer pour l'année 2015 le nombre d'élèves en retard à l'entrée en sixième.

3- Calculer pour chaque année, la part des élèves en retard à l'entrée en sixième. Représenter graphiquement les résultats obtenus et donner un titre informatif.

4- Représenter sous forme de tableau les données de la figure 5 et commenter.

5- Donner une estimation du nombre de garçons et du nombre de filles ayant au moins un an de retard à l'entrée en sixième en 2015.
Aide : Soient X le nombre de filles inscrites en 6e, Y le nombre de garçons inscrits en 6e, X_r le nombre de filles de 6e en retard et Y_r le nombre de garçons de 6e en retard. En utilisant ces variables, écrivez :
- l'équation du nombre d'élève inscrit en 6e.
- l'équation du nombre d'élèves de 6e en retard.
- les équations de calcul du taux de retard à l'entrée en 6e.
- résolvez le système d'équations.

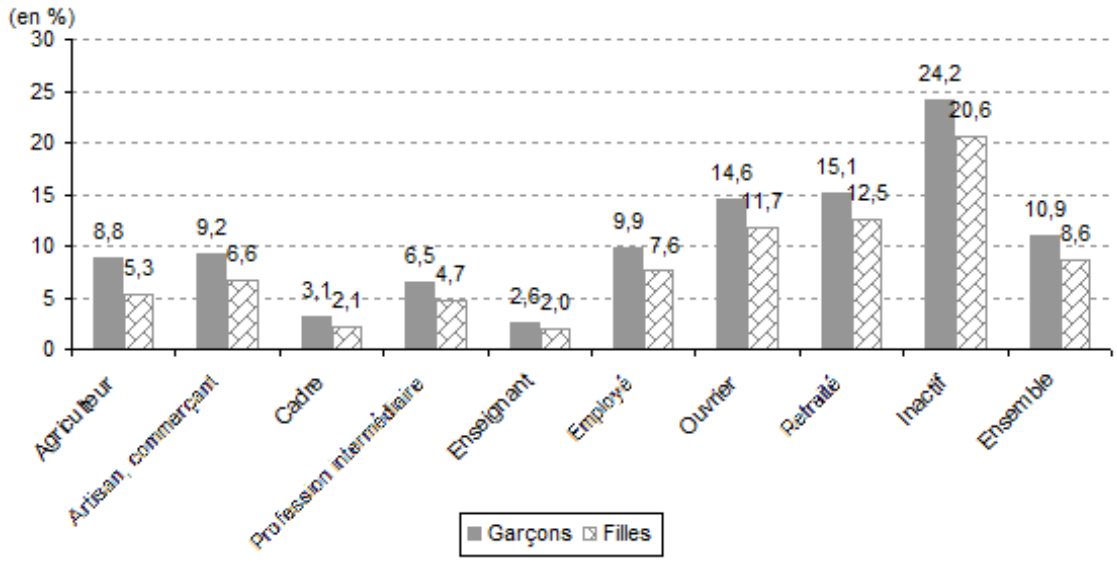
6- À partir des données disponibles, peut-on savoir combien d'enfants de cadre (sans distinction de sexe) sont en retard à leur entrée en sixième en 2015 ? Justifier.

Figure 4 : **Par années, les entrées en sixième**

	2010	2011	2012	2013	2014	2015
« À l'heure » ou en avance	659 401	698 452	695 165	695 083	698 205	710 890
1 an de retard	97 595	95 522	91 741	86 833	79 682	75 327
Au moins 2 ans de retard	2 814	2 805	2 809	2 343	1 775	1 504
Total entrants en sixième	759 810	796 779	789 715	784 259	779 662	787 721

Champ : France métropolitaine + DOM y compris Mayotte à partir de 2011, Public + Privé, MENESR.
Source : MENESR DEPP / Système d'information SCOLARITE.

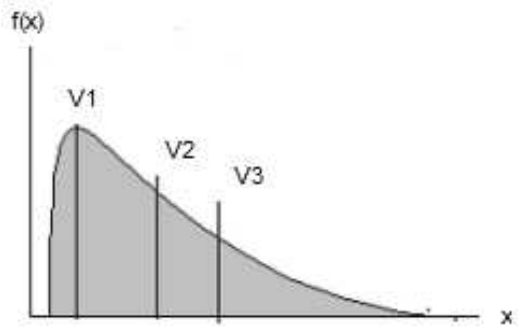
Figure 5 : **Proportion d'élèves en retard à l'entrée en sixième à la rentrée 2015 selon le sexe et l'origine sociale de l'élève**



Champ : France métropolitaine + DOM, MENESR.
Source : MENESR DEPP / Système d'information SCOLARITE.

Exercice 4
(1,5 points)

1- Soit la distribution suivante :



a- Quelle est la nature de la variable représentée ?
b- De V1, V2 et V3 laquelle de ces valeurs représente la moyenne, la médiane et le mode ?

2- Quel indicateur résume le mieux la distribution suivante :
{ 450, 560, 730, 810, 890, 960, 1 020, 13 900 } ? Justifier la réponse.

3- Soient les indicateurs de deux séries distinctes S1 et S2 représentant la taille (en cm) des élèves de deux classes :

	Série S1	Série S2
Moyenne	133,75	133,75
Écart-type	3,74	4,38

Dans quelle série, les valeurs sont-elles le plus homogènes ? Justifier la réponse.
Citer un autre indicateur de dispersion qui aurait pu répondre à cette question.

Exercice 5
(1,5 points)

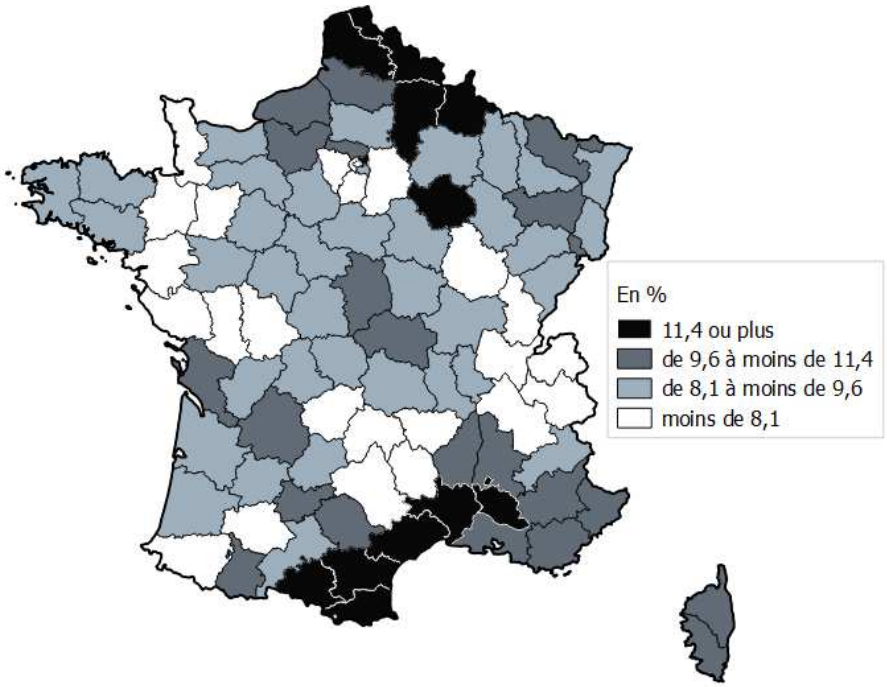
À l'aide des figures 6 et 7, répondre aux questions suivantes :

1- Que signifie le sigle CVS ?

2- Peut-on calculer, à partir des données disponibles, le taux de chômage en Bretagne au 1er trimestre 2017 ?

3- Quelles sont les idées fortes de la figure 6 ?

Figure 6 : **Taux de chômage au 1er trimestre 2017 par département**



Données CVS, en moyenne trimestrielle
Champ : France métropolitaine
Source : Insee, taux de chômage localisés et taux de chômage au sens du BIT

Figure 7 : **Taux (en %) de chômage au 1er trimestre 2017 dans les départements de Bretagne**

Départements	Taux de chômage
Côtes-d'Armor	8,6
Finistère	8,4
Ille-et-Vilaine	7,4
Morbihan	8,6

Données CVS, en moyenne trimestrielle.
Champ : Bretagne.
Source : Insee, taux de chômage localisés et taux de chômage au sens du BIT.

Insee
Mesurer pour comprendre
Direction générale

CONCOURS INTERNE DE CONTRÔLEUR DE L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES

ANNÉE 2019

ÉPREUVE DE RÉDACTION ADMINISTRATIVE

Décembre 2018
(durée : 3 heures, coefficient : 6)
Le sujet comporte 23 pages (y compris celle-ci)

CINRA19P

À partir des seuls documents joints, vous rédigerez une note de synthèse de quatre pages dans laquelle vous décrirez la situation des entreprises françaises face à l'insécurité des systèmes d'information et les moyens mis en place pour y remédier au niveau national et international.

Nota : Il sera tenu compte dans la notation de la clarté de la rédaction, de l'orthographe, de la grammaire et de la présentation

Document 1

P. Lasbordes, **La sécurité des systèmes d'information : un enjeu majeur pour la France**, *Rapport officiel au Premier ministre, La Documentation française, janvier 2006, 195 pages.*

Extrait, pp.63-69

Comment sont organisés nos principaux partenaires étrangers ?

Les ressources humaines des agences homologues de la DCSSI, peuvent être considérées comme un bon indicateur de la priorité politique accordée à ces questions : environ 3000 personnes à la *Division Information Assurance* de la NSA aux États-Unis, 450 au *Bundesamt für Sicherheit in der Infromationstechnik (BSI)* en Allemagne et 450 au C*ommunications Electronics Security Group (CESG)* au Royaume-Uni, contre à peine 110 à la DCSSI. Disposant de plus de moyens que la DCSSI, ces agences développent un véritable partenariat privé-public centré sur les produits de sécurité.
De manière générale, la conception et l'organisation anglo-saxonne de la sécurité des systèmes d'information se caractérisent par une approche unifiée des aspects défensifs et offensifs.

Les États-Unis : une doctrine forte, l'Information dominance

Une agence offensive et défensive la National security agency (NSA)

L'Executive order 12 333 du 4 décembre 1981 décrit les principales responsabilités de la NSA (National security agency créée le 4 novembre 1952). : *« The ability to understand the secret communications of our foreign adversaries while protecting our own communications, a capability in which the United States leads the world, gives our nation a unique advantage »*[1].
Tout est dit en quelques mots sur le pouvoir que revêtent la maîtrise et la protection de son information pour un État. La NSA a une double mission : protéger les systèmes d'information des États-Unis et obtenir des renseignements à partir d'interceptions et des écoutes d'autres pays. La NSA est à la fois une agence de cryptologie et une agence de renseignement. Elle emploie 3500 personnes et son budget n'est pas connu.

L'Information Assurance a pour missions de :

– fournir des solutions, des produits et des services;
– de mener des opérations de protection des systèmes d'information;
– d'assurer la protection des infrastructures critiques au profit des intérêts de la sécurité nationale des États-Unis. *L'Information Assurance Directorate (IAD)*, est l'homologue de la DCSSI du SGDN.

La NSA mène des travaux sur l'instauration de mécanismes d'alerte face aux menaces sur les systèmes d'information et sur le renforcement de la protection des infrastructures vitales fondé sur la mise en oeuvre d'un partenariat étroit avec l'industrie.
Le Directeur de la NSA est un général de corps d'armée.
Après les attentats du 11 septembre 2001, qui ont ébranlé l'image de marque de la NSA, la cybersécurité est devenue un enjeu de sécurité nationale fondé sur la définition de la stratégie nationale de sécurisation du cyberspace (National Strategy to Secure Cyberspace) du Critical Infrastructure Protection Board.

L'USA PATRIOT ACT, promulgué en octobre 2001, invite à la mise en oeuvre d'actions nécessaires à la protection des infrastructures critiques, actions développées sous la responsabilité de

1 « La capacité à comprendre les communications secrètes de nos adversaires étrangers tout en protégeant nos propres communications, une aptitude dans laquelle les États-Unis sont les leaders mondiaux, confère un avantage unique à notre nation. »

partenariats public-privé. L'Office of Homeland Security (OHS) est établi par l'executive order 13 228 et est chargé de coordonner les efforts de protection des infrastructures critiques.

Prise en compte de la menace : **veille, alerte, réponse** : la création du Department of Homeland Security par regroupement d'agences auparavant dispersées est un premier pas. Les responsabilités du DHS en matière de sécurité du cyberespace concernent la direction Information Analysis and Infrastructure Protection and Directorate (IAIP) chargée de :
– développer un plan national de sécurisation des infrastructures critiques;
– mettre en place un dispositif de réponses aux attaques sur la sécurité les systèmes d'information critiques;
– assurer une assistance technique au secteur privé et aux administrations dans le cadre d'incidents sur les systèmes d'information critiques et coordonner la diffusion d'informations d'alerte et de protection;
– encourager la recherche dans ces domaines techniques.

L'IAIP s'articule autour du National Infrastructure Protection Center (NIPC) qui couvre l'ensemble des menaces sur les infrastructures critiques et de la National Cyber Security division (NCSD) dont les missions sont l'identification des risques et l'aide à la réduction des vulnérabilités des systèmes d'information gouvernementaux et le développement de l'information sur la cybersécurité de l'ensemble de la société (universités, consommateurs, entreprises et communauté internationale). En mars 2003, le CERT Fédéral du FBI (FedCIRC) a été rattaché au DHS. Il a vocation à traiter prioritairement les administrations civiles.

Royaume-Uni : un partenariat public-privé très développé

En 2003, le Royaume-Uni s'est doté d'une stratégie nationale en matière de sécurité de l'information qui met l'accent sur le partenariat avec le secteur privé et comporte un volet plus particulièrement orienté sur l'information des entreprises et des usagers afin de faire régner l'ordre dans le cyberespace. Le Gouvernement a créé le Central Sponsor Information Assurance (CSIA).

Le Communications and Electronic Security Group (CESG) placé sous l'autorité du Communication *Government Head Quarter*, chargé de la protection des systèmes d'information de l'État, est l'homologue de la DCSSI. Au Royaume Uni, le NISCC[2], rattaché au Home Office, s'appuie sur l'UNIRAS (CSIRT gouvernemental) pour fournir aux opérateurs des infrastructures critiques des avis techniques, des informations sur les menaces, les vulnérabilités et les niveaux d'alerte. Il s'appuie aussi sur des WARP[3], chargé de recueillir des alertes et de signaler des incidents (mais sans capacité d'intervention) et des ISAC[4], qui diffusent des informations d'alerte et d'incident au sein d'une communauté donnée d'utilisateurs, généralement sur une base commerciale.

Un partenariat public-privé très développé : en 1999, le Royaume-Uni a créé, à l'initiative de plusieurs administrations, le National Infrastructure Security Co-ordination Centre (NISCC) qui englobe des missions plus larges liées à la gestion des risques telles que la protection des infrastructures critiques ou le partenariat avec l'industrie.

Le partenariat entre le secteur public et le secteur privé sur l'analyse des vulnérabilités des infrastructures vitales est érigé en système bien défini et s'organise autour de groupes composés de 30 personnes chargés de mettre en place l'échange d'informations. Le NISCC a mis en place des groupes pour 4 secteurs prioritaires : les finances, la sécurité des réseaux, les services externalisés des ministères et les systèmes de supervision de contrôles industriels (SCADA – Supervisory Control and Data Acquisition). Les secteurs des compagnies aériennes, des opérateurs d'Internet et des distributeurs feront l'objet du même plan d'action. Par ailleurs, le NISCC a formalisé avec les éditeurs de produits un protocole d'accord sur le partage

2 National Infrastructure Security Co-ordination Centre.
3 Warning, Advice and Reporting Point.
4 Information Sharing and Analysis Center.

d'informations sur les vulnérabilités articulé autour de neuf principes, dont l'objectif principal est de garantir la confidentialité absolue des informations transmises par le NISCC.

Le ministère de l'Économie et de l'Industrie poursuit sa procédure de tests fonctionnels des produits de sécurité, nommée GIPSI[5] et a émis deux premiers certificats (le niveau d'exigence est moins élevé que pour les certificats critères communs). Au CESG, les travaux se poursuivent sur le passeport électronique (délivrance des clés et évaluation du dispositif) pour une délivrance des premiers passeports à l'automne 2006. Par ailleurs, un nouveau programme de recherche (IADP 1) a été mis en place afin d'optimiser les efforts dans le domaine SSI, en partenariat avec l'industrie.

Allemagne : une politique produit forte, très tournée vers les utilisateurs

L'Allemagne a adopté en juillet dernier, un plan national pour la protection des infrastructures d'information (NPSI)[6] qui comporte trois objectifs principaux :

– la prévention afin de protéger convenablement les infrastructures;
– la préparation afin de répondre efficacement en cas d'incidents de sécurité informatique;
– le maintien et le renforcement des compétences allemandes dans le domaine SSI.

Ce plan doit être maintenant décliné sous la forme de plans d'actions plus détaillés permettant sa mise en place dans le secteur public et dans le secteur privé qui est très concerné car il détient une grande partie des réseaux de communication.

La mise en oeuvre de ce plan s'appuiera notamment sur le BSI, rattaché au ministère de l'Intérieur, qui est responsable de la SSI en Allemagne, homologue de la DCSSI. Il compte un effectif de 430 personnes (contre 100 à la DCSSI) en croissance régulière depuis 2001.

Les objectifs du BSI sont de sécuriser les systèmes d'information allemands.
Pour les atteindre, le BSI assure, auprès des utilisateurs quels qu'ils soient (administration, entreprises, citoyens) et des fabricants de technologies de l'information les missions suivantes :

– Informer le pays :
• en sensibilisant le public aux enjeux de la SSI par exemple par une information trimestrielle sur leur site Web et la production de CD-rom conçus pour les citoyens. L'industrie supporte cette initiative du BSI et fournit gratuitement des démonstrateurs;
• en participant à des campagnes de sensibilisation des PME en 2004 (Sécurité de l'Internet pour les PME);
• le BSI réalise également des analyses de tendance et des futurs risques qui pèsent sur les systèmes d'information.

– Fournir des conseils et des supports techniques dans le cadre d'un partenariat avec le privé très fort :
• ainsi le BSI a créé un standard professionnel en 1993, une IT Baseline Protection (les bases de la protection d'un système d'information) remise à jour constamment qui est devenu un standard pour l'industrie. C'est un ensemble de bonnes pratiques qui permettent de sécuriser un système (CD-ROM ou 3 classeurs papier). Au départ, des grandes entreprises allemandes (SIEMENS, DAIMLER, VW, des banques...) se sont associées à cette initiative. La baseline protection est utilisée par le gouvernement et par les entreprises ;
• il assure du conseil et un support technique en sécurité des SI vers les agences gouvernementales par exemple l'initiative 2005 BundOnline ou la justice et la police;

5 General InformationAssuranceProducts andServices Initiative – www.gipsi.gov.uk
6 http://www.bmi.bund.de/nn_148134/Internet/Content/Nachrichten/Pressemittteilungen/2005/08/Information__Infrastructure__en.html .

• il réalise des tests d'intrusion et apporte l'expertise sur la protection contre les bogues et les émissions radios. Ainsi, le BSI a une équipe spécialisée qui réalise des tests d'intrusion pour les ministères et les entreprises des secteurs sensibles;
• la protection des infrastructures critiques est confiée au BSI qui a entrepris un travail d'identification de ces infrastructures, grâce à des exercices impliquant l'administration (ministères de l'Intérieur, de la Défense, des Transports, des Télécommunications) et des industriels. Dans ce cadre, il entretient des relations avec d'autres pays comme les États-Unis, la Suisse, la Suède et la Finlande;
• le BSI conseille également les Länder sur le plan technique.

– Analyser les risques, évaluer et tester :
• le BSI assure la certification des produits et services de SSI (38 en 2004) ainsi que l'attribution de licences pour des applications classifiées;
• il a une action particulière sur les procédures biométriques et des applications mobiles;
• il conduit une analyse permanente de la sécurité Internet et de ses évolutions.
Par exemple le BSI a une équipe spécialisée sur le projet de l'alliance TCG (Trusted Computing Group) qui a des relations avec TCG mais qui recherche aussi des alternatives.

– Développer des produits et des technologies SSI :
Le BSI évalue et développe des équipements cryptographiques ainsi que des outils de sécurité et de modèles de sécurité formelle. Ainsi, le BSI participe à des projets à forte implication technologique : la carte santé (18 millions de cartes) la CNI-e avec 80 millions de cartes (carte d'identité) ou encore le passeport biométrique.

– Assurer des fonctions opérationnelles :
• assurer la fonction de CERT allemand (Computer Emergency Response Team) ;
• coordination technique du réseau d'information Berlin-Bonn ;
• administration de la PKI du gouvernement ;
• production de clés pour les équipements cryptographiques
.
– Jouer un rôle actif dans la normalisation et la standardisation:
Le BSI joue un rôle actif dans les comités nationaux et internationaux de normalisation et de standardisation relatifs à la SSI. Pour assurer l'ensemble de ces missions, le BSI dispose d'un budget significatif de 51 millions d'euros en augmentation régulière depuis 2002. La répartition de ce budget, montre une action forte sur les développements, 10 M€, soit 19 % du budget et les études pour 9 M€ soit 17 % du budget que l'on ne retrouve pas en France.

Enfin, l'enquête de satisfaction réalisée par TNS-Emnid auprès de 500 experts de SSI afin de juger la qualité de cette politique volontariste du BSI, indique que 86 % des sondés sont satisfaits de son travail. La réputation très forte du BSI en Allemagne est une réalité.

Document 2

Sécurité informatique : les entreprises doivent se préparer à être confrontées à de nouveaux risques

Le journal du net - Chronique de Florian Malecki – 30/04/15

Tandis que l'Internet des Objets devient une réalité tangible, que les systèmes mobiles s'enrichissent en fonctionnalités et offrent de nouveaux moyens d'interaction, il faut se rendre à l'évidence : la sécurité IT reste problématique.

L'irruption des nouvelles technologies dans notre quotidien offre d'importants bénéfices, tant aux particuliers qu'aux entreprises. Mais ces innovations comportent également leur lot de risques. Il devient évident que les entreprises et les départements informatiques doivent administrer aussi judicieusement qu'efficacement leurs infrastructures et leurs applications pour se protéger contre les attaques externes. Et il existe une grande variété de solutions de sécurité en mesure de répondre au large éventail de menaces.

Mais la sécurité informatique exige également la mise en place de process et de politiques de sécurité. Les entreprises doivent en permanence s'adapter à de nouvelles menaces. Lors du dernier salon CeBIT, l'un des plus grands rassemblements autour des technologies, la sécurité IT était un enjeu essentiel. De plus, à en croire les nombreuses conversations que nous avons eues avec nos clients et partenaires, la sécurité de leurs infrastructures IT s'avère être pour eux une préoccupation majeure.

Dell a récemment identifié les six principaux domaines dans lesquels les entreprises pourront s'attendre à observer un accroissement rapide du nombre de menaces de sécurité :

1. L'Internet des Objets

L'Internet des Objets va inévitablement générer de nouveaux risques en matière de sécurité. Avec les progrès de la domotique, chaque foyer devrait abriter à terme entre 50 et 100 objets connectés avec des risques critiques liés à la vie privée.

Bien que les avertissements selon lesquels les réfrigérateurs et les télévisions connectés sont vulnérables aux hackers paraissent exagérés, en 2015 les entreprises pourront s'attendre à voir augmenter le nombre de ces attaques. L'importance du phénomène s'accroît lorsque les équipements constitutifs de l'Internet des Objets ne répondent pas aux standards basiques de sécurité.

2. Les appareils mobiles

Les attaques relatives aux terminaux mobiles continueront également à augmenter. Bien que la grande majorité des malwares pour ces types d'appareils repose sur le système d'Android, il n'est pas totalement exclu que les systèmes iOS pourront eux aussi être affectés.

3. Cybercriminalité

Le nombre de cyberattaques apparaît également en hausse. Les motivations de ces cyberattaques varient : elles peuvent être économiques ou politiques. Les données de cartes bancaires sont aussi visées ainsi que les infrastructures critiques d'établissements publics, y compris les réseaux SCADA. Dell a en effet constaté une forte hausse des attaques des systèmes SCADA de ses clients durant l'année 2014 (deux fois plus qu'en 2013). Sur les sites industriels, les systèmes SCADA sont utilisés pour contrôler les équipements à distance et pour collecter des données sur les performances des équipements. Les attaques des systèmes SCADA en progression sont de nature politique car elles ciblent les capacités opérationnelles de centrales, d'usines et de raffineries. Les attaques par « débordement de la mémoire tampon » (« buffer overflow ») restent le moyen d'attaque le plus courant.

4. Machines virtuelles

Les machines virtuelles sont exposées aux mêmes risques que les serveurs physiques mais leur flexibilité et leur approche orientée applications les soumets à des menaces supplémentaires.

Les entreprises choisissent de plus en plus de virtualiser leur infrastructure et le nombre d'attaques contre les environnements virtuels, attaques perpétrées à l'aide de malwares spécialement conçus pour cet usage, augmente également.

5. Code ancien, vulnérabilités nouvelles

Même un code ancien peut héberger des vulnérabilités. Les attaques Unix-Shell Bash ou Heartbleed Open SSL en ont récemment fourni la preuve. Ce type de vulnérabilité continuera de constituer une menace pour les réseaux.

6. Distributeurs automatiques de billets et de tickets / Terminaux points de vente

Bien que les guichets et distributeurs de billets soient souvent équipés de systèmes sécurisés, le vol de données de cartes bancaires reste une activité lucrative pour les criminels.

Par ailleurs, l'industrie de la vente au détail a été sérieusement ébranlée en 2014 après que plusieurs chaînes de la grande distribution ont été victimes de violations sur le point de vente (POS), exposant des millions de consommateurs aux risques d'être victimes d'achats frauduleux ou de vol d'identité. Les malwares qui s'attaquent aux systèmes sur le point de vente évoluent et de nouvelles tendances se dessinent, avec le recours aux techniques de « memory scraping » ou au chiffrement pour tromper les pare-feu.

7. Augmentation des attaques via le trafic censé être sécurisé par le protocole web HTTPS

Pendant de nombreuses années, les institutions financières et d'autres sociétés amenées à traiter des informations sensibles ont opté pour le protocole de sécurité HTTPS de chiffrement des échanges d'information, également appelé chiffrement SSL/TLS. Cédant à la pression des utilisateurs et répondant ainsi à leurs réclamations répétées de sécurité et de protection de la vie privée, des services en ligne comme Google, Facebook et Twitter se sont mis à implémenter ces protocoles. Mais si l'adoption d'un protocole web mieux sécurisé va dans le bon sens, les pirates ne sont pas en reste et s'efforcent de cacher du code malveillant dans le protocole HTTPS. Comme les données (ici le code du malware) transmises par HTTPS sont chiffrées, les pare-feu traditionnels peinent à les détecter.

Afin de réduire les risques de sécurité qui sont en pleine croissance, les entreprises doivent repenser leurs stratégies de sécurité et s'y adapter. Adopter une approche intégrée de la sécurité est un bon premier pas. Les infrastructures en silo existantes sont clairement un frein à cette volonté d'améliorer la sécurité des systèmes. Pour répondre aux attaques composites complexes à plusieurs niveaux, seules des solutions de bout en bout sont efficaces, puisqu'elles permettent de combler les lacunes tant au niveau des serveurs et des réseaux qu'au niveau des terminaux informatiques de tous acabits.

Document 3

Insee Première

N° 1594

Mai 2016

Sécurité numérique et médias sociaux dans les entreprises en 2015

En 2015, parmi les sociétés de 10 personnes ou plus implantées en France, 27 % déclarent avoir une politique de sécurité des technologies de l'information et de la communication (TIC) formellement définie ; elles sont 32 % au niveau européen. En France comme dans l'Union européenne (UE à 28), les trois quarts des sociétés de 250 personnes ou plus sont dans ce cas.

En France, 13 % des sociétés de 10 personnes ou plus ont subi au moins un incident de sécurité au cours de l'année précédente, portant atteinte à l'intégrité, à la disponibilité ou à la confidentialité des systèmes et données informatiques. Les sociétés de 250 personnes ou plus sont deux fois plus touchées. Pour sécuriser leur réseau informatique, les trois quarts des sociétés de 10 personnes ou plus utilisent un pare-feu ou un logiciel de protection de l'accès à distance. Par ailleurs, un quart déclare avoir une politique d'accès, de rectification et d'effacement des données personnelles.

En 2015, 16 % des sociétés de 10 personnes ou plus implantées en France emploient du personnel spécialisé dans le domaine des TIC ; elles sont 20 % au niveau européen. Les plus grandes sociétés le font beaucoup plus fréquemment, tandis que les plus petites font souvent appel à des prestataires externes.

Entre 2013 et 2015, l'usage des médias sociaux a progressé de 11 points dans les sociétés de 10 personnes ou plus implantées en France, mais reste inférieur à celui de l'UE à 28 (31 % contre 39 %). Par ailleurs, en 2015 comme en 2013, les deux tiers des sociétés disposent d'un site web. En 2015, une société sur trois de 10 à 49 personnes n'a ni site web, ni compte sur un média social, contre seulement une sur dix pour celles de 50 personnes ou plus.

Elvire Demoly, Thomas Vacher, division Enquêtes thématiques et études transversales, Insee

La sécurité dans le domaine des technologies de l'information et de la communication (TIC) implique des mesures, contrôles et procédures pour garantir l'intégrité, la confidentialité ainsi que la disponibilité des données et des systèmes d'information. Elle constitue un enjeu majeur pour les entreprises, du fait de la diffusion du numérique. Un incident, une défaillance ou une attaque peuvent avoir de lourdes conséquences, pour l'entreprise ou pour ses clients notamment.

Trois quarts des « grandes » sociétés ont une politique de sécurité des TIC

En 2015, en France, 27 % des sociétés de 10 personnes ou plus déclarent avoir une politique de sécurité des TIC formellement définie. Ce niveau est proche de celui de l'Allemagne (29 %), mais inférieur à celui de l'Union européenne (UE à 28, 32 %). En Lituanie et en Suède, c'est le cas pour plus de la moitié des sociétés. En France, comme dans l'UE à 28, la moitié des sociétés de 50 à 249 personnes et les trois quarts des « grandes » sociétés, celles de 250 personnes ou plus, ont une politique de sécurité des TIC formellement définie.

Les sociétés où les TIC sont au cœur de l'activité sont aussi plus concernées. Ainsi, la moitié des sociétés de l'information-communication et des activités scientifiques et techniques le sont, contre respectivement une sur sept et une sur six dans la construction et l'hébergement-restauration *(figure 1)*.

Trois types de risques pris en compte par la politique de sécurité des TIC sont considérés ici : celui sur l'intégrité des données (destruction ou altération de données due à une attaque ou à un incident inattendu), celui sur la confidentialité des données (divulgation de données confidentielles due à une intrusion, à des attaques par *pharming*, *phishing* *(définitions)* ou par accident) et celui sur la disponibilité des services (indisponibilité des services TIC due à une attaque extérieure, par déni de service *(définitions)* par exemple). Lorsqu'une politique de sécurité des TIC est définie, elle prend en compte neuf fois sur dix l'intégrité des données,

huit fois sur dix leur confidentialité et sept fois sur dix la disponibilité des services.
Pour être efficace, une politique de sécurité peut nécessiter une actualisation régulière afin de l'adapter aux évolutions des systèmes, aux incidents passés et aux risques nouveaux. Ainsi, 20 % des sociétés de 10 personnes ou plus ont défini ou actualisé leur politique de sécurité des TIC au cours des deux années précédant l'enquête, soit les trois quarts de celles qui prennent ces mesures de sécurité.

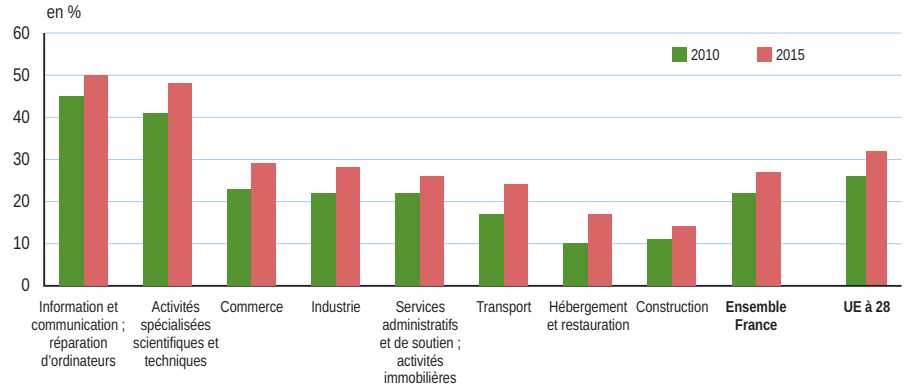
Un quart des « grandes » sociétés ont subi un incident de sécurité informatique

En 2015, en France, 13 % des sociétés de 10 personnes ou plus déclarent avoir subi, au cours de l'année précédente, au moins un incident de sécurité portant atteinte à l'intégrité, à la disponibilité ou à la confidentialité des systèmes et données informatiques, soit 4 points de plus qu'en 2010 *(figure 2)*. Cette hausse peut être due à l'expansion des équipements TIC.
Ces incidents concernent plus souvent les sociétés les plus grandes et celles des secteurs d'activité en lien fort avec les TIC, en raison de leur taux plus élevé d'équipement et d'usage des TIC. Ainsi, 24 % des sociétés de 250 personnes ou plus déclarent au moins un incident de sécurité au cours de l'année 2014 ; c'est deux fois plus que pour celles de 10 à 49 personnes (12 %).
Les incidents les plus répandus sont les pannes de logiciel ou de matériel informatique, qui entraînent l'indisponibilité des services, la destruction ou l'altération des données (8 % des sociétés de 10 personnes ou plus). Viennent ensuite les attaques de programmes malveillants, comme les virus, ou les accès non autorisés, qui aboutissent à la destruction ou à l'altération de données (7 %). Seules 3 % des sociétés de 10 personnes ou plus déclarent avoir subi des attaques extérieures, par exemple par déni de services, et 2 % des attaques par intrusion, *pharming* ou *phishing* ayant abouti à la divulgation de données confidentielles. Ces chiffres sont sans doute sous-estimés, car certaines sociétés sont réticentes à évoquer ce type d'incident.

Le pare-feu très souvent utilisé pour sécuriser le réseau informatique

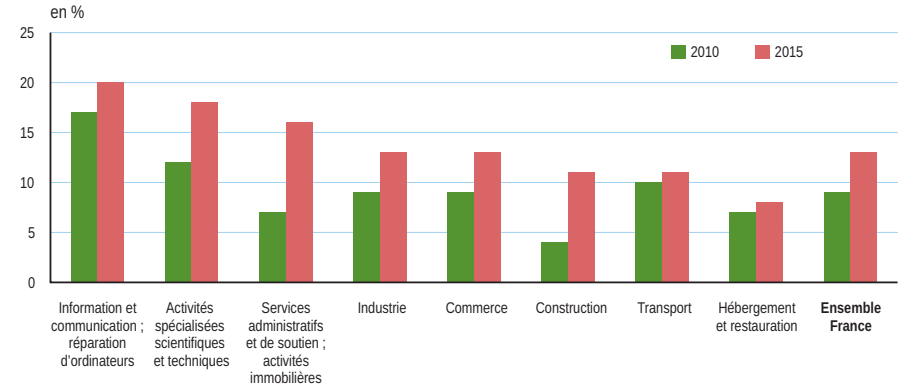
Divers moyens existent pour sécuriser l'accès aux données importantes présentes sur le système informatique d'une entreprise, qu'il s'agisse de données générées par l'activité de l'entreprise, de données à caractère personnel (fichiers de clients, de salariés, etc.) ou de données couvertes par le secret industriel par exemple. En 2015, sept sociétés sur dix de 10 personnes ou plus, mais la quasi-totalité des grandes sociétés, utilisent le contrôle de l'accès à distance par pare-feu *(firewall)* ou logiciel. La moitié des sociétés de 10 personnes ou plus sécurisent les équipements mobiles *via* le contrôle par mot de passe, l'effacement des données stockées sur les appareils en cas de perte ou de vol ; les trois quarts des grandes sociétés le font. Enfin, le quart des sociétés de 10 personnes ou plus contrôle l'accès physique aux serveurs (par badge, biométrie, etc.) ; les trois quarts des grandes, mais seulement le cinquième des petites (10 à 49 personnes) exercent ce contrôle. Toutes les sociétés qui contrôlent l'accès physique aux serveurs utilisent aussi un pare-feu ou logiciel de contrôle à distance.

1 Sociétés ayant une politique de sécurité des TIC formellement définie



Champ : sociétés de 10 personnes ou plus, implantées en France et dans l'UE à 28, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Sources : Insee, Eurostat, enquêtes TIC 2010 et 2015.

2 Sociétés ayant subi au moins un incident informatique au cours de l'année précédente



Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquêtes TIC 2010 et 2015.

Une politique d'accès aux données personnelles dans un quart des sociétés

La loi Informatique et libertés de 1978 donne le droit à toute personne d'accéder aux données la concernant et figurant dans un fichier informatique. Celle-ci peut également demander au responsable de ce fichier la rectification ou l'effacement de ces données.
En 2015, en France, 26 % des sociétés de 10 personnes ou plus déclarent avoir une politique d'accès, de rectification et d'effacement des données personnelles. Cette proportion est de 62 % parmi les sociétés de 250 personnes ou plus et de 48 % parmi celles du secteur de l'information et de la communication de 10 personnes ou plus *(figure 3)*.
Quels que soient l'effectif de l'entreprise ou son secteur d'activité, certains usages des TIC impliquent souvent le traitement de données personnelles permettant d'identifier une personne physique, directement ou indirectement. C'est le cas de la vente web, de l'utilisation des médias sociaux ou de la gestion des relations avec les

3 Sociétés ayant une politique d'accès, de rectification et d'effacement des données personnelles

Parmi les sociétés :	Part (en %)
De 10 à 49 personnes	23
De 50 à 249 personnes	41
De 250 personnes ou plus	62
Industrie	25
Construction	15
Commerce	29
Transport	24
Hébergement et restauration	21
Information et communication ; réparation d'ordinateurs	48
Activités spécialisées scientifiques et techniques	36
Services administratifs et de soutien ; activités immobilières	30
Faisant de la vente web	38
Utilisant les médias sociaux	38
Utilisant un CRM / GRC *	40
Ensemble	**26**

* Outils de gestion des relations avec la clientèle.
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquête TIC 2015.

clients. Les sociétés concernées par ces usages déclarent plus souvent avoir une politique d'accès, de rectification et d'effacement des données personnelles.

Six sociétés sur dix sensibilisent leur personnel à la sécurité des données

Sans avoir forcément de politique formelle autour de la sécurité des TIC, six sur dix des sociétés implantées en France de 10 personnes ou plus déclarent sensibiliser leur personnel à ses devoirs concernant les problèmes de sécurité sur les données, au travers notamment de clauses contractuelles ou d'engagement ou par des formations. La moitié des sociétés sensibilisent à la fois à la sécurité des données à caractère personnel (notamment sur leurs clients ou salariés) et à celle des données d'entreprise, concernant la propriété intellectuelle par exemple. Les sociétés qui ont une politique de sécurité formellement définie sensibilisent plus souvent (huit sur dix) leur personnel à la sécurité des données.

Les grandes sociétés ont leurs spécialistes en TIC, les petites sous-traitent

En 2015, 16 % des sociétés implantées en France de 10 personnes ou plus emploient du personnel spécialisé dans le domaine des TIC, c'est-à-dire des personnes dont l'activité principale consiste à développer, faire fonctionner ou maintenir des systèmes d'information ou des applications informatiques. Cette part est de 20 % dans l'UE à 28. En France, comme dans l'UE à 28, 77 % des sociétés de 250 personnes ou plus en emploient.

Les écarts selon l'effectif des sociétés sont plus faibles dans les secteurs proches des TIC. Ainsi, dans le secteur de l'information et de la communication, la totalité des grandes sociétés de 250 personnes ou plus emploie des spécialistes, et plus de sept sur dix parmi les petites sociétés de 10 à 49 personnes. En revanche, dans l'hébergement et la restauration, les trois quarts des grandes sociétés, mais très peu de petites (4 % seulement) emploient des spécialistes en TIC.

Qu'elles emploient ou non des spécialistes, les sociétés sous-traitent fréquemment certaines opérations liées aux TIC. Ainsi, en 2014, 62 % des sociétés de 10 personnes ou plus ont principalement fait appel à un prestataire externe pour la maintenance des infrastructures (serveurs, ordinateurs, imprimantes, réseaux) et 53 % pour des opérations relatives à la sécurité et la protection des données. En revanche, les traitements de données et les fonctions support de bureautique sont plus fréquemment assurés principalement par le personnel de la société *(figure 4)*.

Toutefois, les grandes sociétés, majoritairement employeuses de spécialistes en TIC, comptent plus de travaux principalement effectués par leurs propres employés *(figure 5)*.

Les médias sociaux de plus en plus utilisés par les sociétés

Les médias sociaux désignent quatre types d'applications internet : les réseaux sociaux (Facebook, LinkedIn, Xing, Viadeo, Yammer, Google+, etc.), les blogs d'entreprise ou les microblogs (Twitter, Present.ly, etc.), les sites web de partage de contenus multimédias (Youtube, Flickr, Picasa, Slideshare, etc.) et les wikis et autres outils de partage des connaissances.

En deux ans, l'usage des médias sociaux a nettement progressé. En 2015, en France, 31 % des sociétés de 10 personnes ou plus disposent d'un profil, d'un compte ou d'une licence d'utilisateur pour accéder à un ou plusieurs médias sociaux contre 20 % en 2013. Dans l'UE à 28, elles sont 39 % contre 30 % en 2013. Les réseaux sociaux demeurent de loin les médias sociaux les plus utilisés : 29 % des sociétés de 10 personnes ou plus y ont recours (18 % en 2013) contre 9 % pour les blogs, 9 % pour les sites web de contenu multimédia et 4 % pour les wikis *(figure 6)*.

L'usage des médias sociaux progresse plus vite dans les sociétés de 50 personnes ou plus (+ 14 points entre 2013 et 2015) que dans celles de 10 à 49 personnes (+ 9 points). En 2015, 57 % des sociétés de 250 personnes ou plus s'en servent.

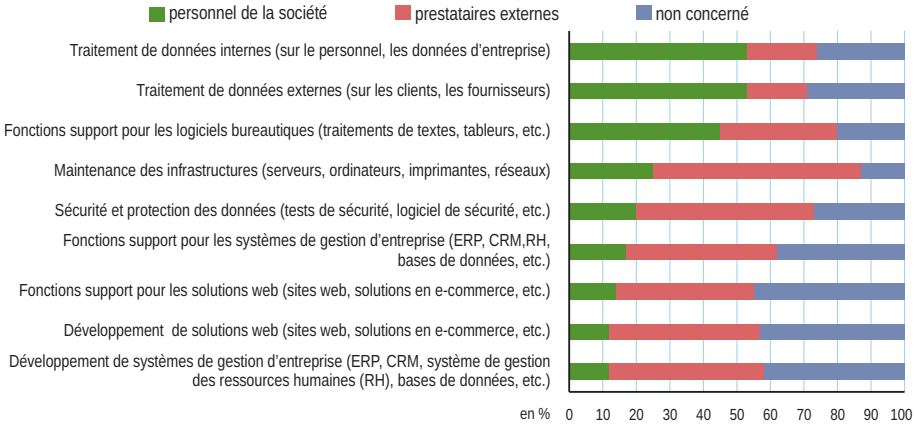
Les secteurs de l'information, de la communication et de la réparation d'ordinateurs restent en tête : 74 % des sociétés y utilisent les médias sociaux en 2015 *(figure 7)*. L'usage est également fréquent dans l'hébergement et la restauration (51 %). Les transports et la construction restent en retrait (moins de 20 %).

Comme en 2013, le principal motif d'utilisation est de développer l'image de l'entreprise ou commercialiser ses produits (9 sociétés sur 10) et le second de recueillir l'avis, les critiques ou les questions des clients ou y répondre.

Un tiers des petites sociétés ne s'affichent pas sur la toile

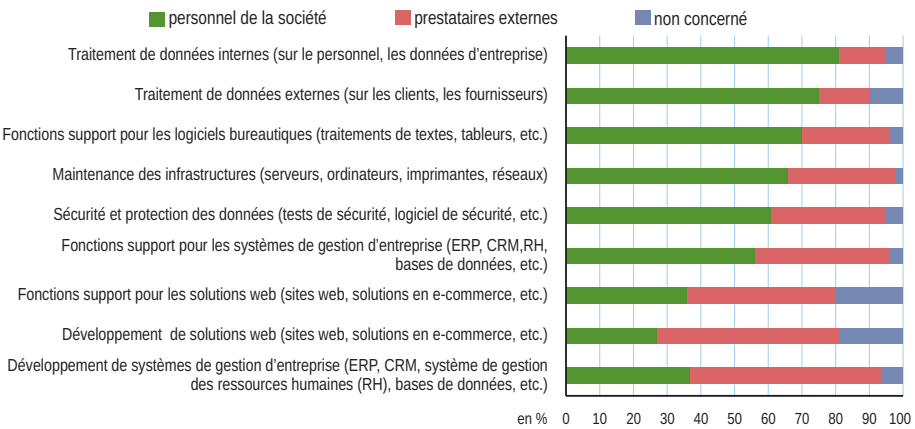
Autre moyen de s'afficher sur Internet, le site web reste beaucoup plus utilisé que les médias sociaux, sans toutefois progresser beaucoup. En 2015, 67 % des sociétés implantées en France de 10 personnes ou plus disposent d'un site web ou d'une page d'accueil. C'est 8 points de moins que la moyenne européenne, mais l'écart n'est dû qu'aux sociétés de 10 à 49 personnes : en France, 63 % d'entre elles ont un site web ou une page d'accueil

4 Les opérations TIC dans les sociétés de 10 personnes ou plus réalisées principalement par…



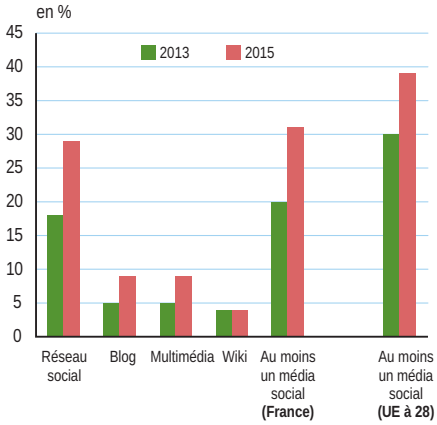
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquête TIC 2015.

5 Les opérations TIC dans les sociétés de 250 personnes ou plus réalisées principalement par…



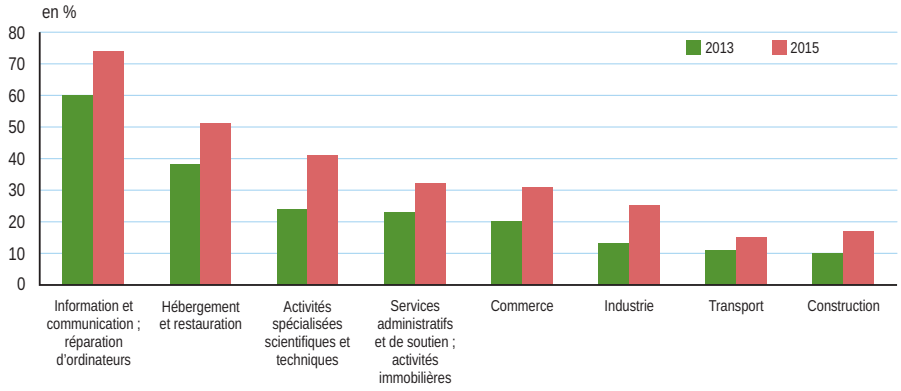
Champ : sociétés de 250 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquête TIC 2015.

6 Utilisation des médias sociaux



Champ : sociétés de 10 personnes ou plus, implantées en France ou dans l'UE à 28, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Sources : Insee, Eurostat, enquêtes TIC 2013 et 2015.

7 Utilisation d'au moins un média social



Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquêtes TIC 2013 et 2015.

contre 72 % au niveau européen. En revanche, parmi les sociétés de 50 personnes ou plus, neuf sur dix en ont un, en France comme en Europe.
Parmi les petites sociétés qui n'ont pas de site web, seule une sur dix utilise par ailleurs un média social. Le tiers des sociétés de 10 à 49 personnes n'a ainsi ni site web, ni compte sur un média social, contre seulement 11 % de celles de 50 à 249 personnes et 5 % de celles de 250 personnes ou plus. ■

Sources

L'enquête sur les technologies de l'information et de la communication et le commerce électronique (TIC) de 2015 a été réalisée début 2015 auprès d'un échantillon de 13 000 unités légales, sociétés ou entreprises individuelles, actives, occupant 10 personnes ou plus (salariés ou non-salariés) et implantées en France. Le terme « sociétés » est utilisé ici pour les désigner de manière générique. Cette étude s'appuie en effet sur la définition juridique de l'entreprise (unité légale), et non sur la définition économique instaurée par la loi de modernisation de l'économie (LME) et son décret d'application n° 2008-1354 du 18 décembre 2008.
L'enquête porte sur les secteurs d'activité suivants : industrie, construction, commerce et réparation d'automobiles et de motocycles, transports et entreposage, hébergement et restauration, information et communication, activités immobilières, activités spécialisées, scientifiques et techniques, activités de services administratifs et de soutien (sections C à J, L, M hors 75, N et groupe 95.1 de la NAF rév.2). L'échantillon est représentatif d'environ 185 000 sociétés.
Parmi les sociétés actives de l'échantillon, 81 % ont répondu à l'enquête. En termes de précision, la proportion de sociétés ayant une politique de sécurité des TIC formellement définie, par exemple, est estimée à 27 % avec un intervalle de confiance à 95 % de 1 point.
L'enquête annuelle sur les TIC vise à mieux connaître l'informatisation et la diffusion des technologies de l'information et de la communication dans les entreprises. Les questions sur les taux d'équipement en TIC portent en général sur la situation au moment de l'enquête, c'est-à-dire au cours du premier trimestre 2015. Celles portant sur certaines pratiques, notamment le commerce électronique, se réfèrent à l'année précédant l'enquête (soit 2014 pour l'enquête 2015).
En 2015, le questionnaire comporte un module spécifique de questions sur la sécurité des TIC, dont certaines avaient été posées en 2010. Des enquêtes analogues ont été menées dans tous les pays européens en application du règlement communautaire n° 1006/2009 sur la société de l'information.

Définitions

Une attaque **par déni de service** (*denial of service attack*, abrégé en DoS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise.
Le ***pharming*** (ou dévoiement en français) est une technique de piratage informatique. Elle consiste à dérouter la circulation d'un site web vers un faux site web, afin d'acquérir des informations.
Le ***phishing*** (hameçonnage ou filoutage en français) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels concernant des internautes dans le but de perpétrer une usurpation d'identité.

Bibliographie

- Pépin J.-M., « Enquête sur les technologies de l'information et de la communication et le commerce électronique 2015 », *Insee Résultats*, série Économie, à paraître.
- « ICT security in enterprises » , *Statistics explained*, Eurostat, décembre 2015.
- Vacher T., Demoly E., « La timide émergence du cloud computing dans les sociétés en 2014 » *Insee Première* n° 1545, avril 2015.
- Vacher T., « L'usage d'Internet par les sociétés en 2013 : un recours minoritaire aux médias sociaux », *Insee Première* n° 1495, avril 2014.

Direction Générale :
18, bd Adolphe-Pinard
75675 PARIS CEDEX 14
Directeur de la publication :
Jean-Luc Tavernier
Rédacteur en chef :
E. Nauze-Fichet
Rédacteurs :
J.-B. Champion, C. Collin,
C. Lesdos-Cauhapé, V. Quénechdu
Maquette : RPV
Impression : Jouve
Code Sage IP161594
ISSN 0997 - 3192

- ***Insee Première*** figure dès sa parution sur le site internet de l'Insee : www.insee.fr/collections-nationales
- Pour recevoir par courriel les avis de parution (50 numéros par an) : http://www.insee.fr/abonnements

Pour vous abonner à ***Insee Première*** et le recevoir par courrier : http://www.webcommerce.insee.fr/liste.php?idFamille=16

Insee
Mesurer pour comprendre

Document 4

P. Lasbordes, **La sécurité des systèmes d'information : un enjeu majeur pour la France**, *Rapport officiel au Premier ministre, La Documentation française, janvier 2006, 195 pages.*

Extrait, pp.13-19 - Synthèse

Sécurité des systèmes d'information :
Un enjeu majeur pour la France

Pour les besoins de ce document, on appelle « système d'information (SI) » un ensemble de machines connectées entre elles de façon permanente ou temporaire permettant à une communauté de personnesphysiques ou morales d'échanger des données (sons, images, textes, etc.). Selon cette définition, des systèmes aussi variés que le réseau d'un opérateur de téléphonie, le site Internet d'un ministère, l'ordinateur individuel du particulier ou le réseau de commandement des forces armées sont des systèmes d'information.

Une menace qui doit être prise au sérieux

L'information gérée par les systèmes d'information fait l'objet de convoitises. Elle peut être exposée à des attaques qui exploitent des éléments vulnérables du système d'information. La sécurité des systèmes d'information a pour objet de contrer ces menaces par des mesures proportionnées aux risques pouvant peser sur la confidentialité de l'information, son intégrité, sa disponibilité ou la possibilité d'en authentifier la source et de la signer.

Les attaques sont une réalité. Les plus médiatisées sont les virus, vers, phising, spyware, ou les défigurations de site Web. Autrefois imputables à quelques agitateurs, elles sont désormais le fait d'organisations criminelles organisées avec des finalités notamment financières.
L'organisation (recours à l'externalisation, absence de classification des informations...), la faiblesse des acteurs humains (inconscience, insouciance, naïveté), les réseaux de communication (risques de saturation, d'interception...), les logiciels dont la complexité croissante est source d'erreurs difficiles à détecter, ou les composants matériels, sont autant de sources de vulnérabilités.

Le risque peut être quantifié : il est fonction de la valeur attachée aux informations manipulées, de l'importance des vulnérabilités et de la probabilité d'exploitation de ces vulnérabilités par un attaquant.

Pour un système donné, le risque peut être réduit en limitant la sensibilité des informations qu'il manipule, en réduisant la vulnérabilité de chaque entité du système et en multipliant les éléments de défense convenablement architecturés pour compliquer la tâche des attaquants potentiels. Il est également nécessaire de mettre en œuvre une politique de sécurité applicable à l'ensemble des entités d'un domaine géographique ou fonctionnel, qui regroupe l'ensemble des règles et des recommandations à appliquer pour protéger les ressources informationnelles.

Les citoyens, les entreprises, le monde académique, les infrastructures vitales et l'État lui-même sont des cibles. Compte tenu de l'interconnexion entre les réseaux, ces cibles sont de plus en plus interdépendantes. Il importe donc de se préoccuper de la sécurité de tous les acteurs.

Les réponses organisationnelles et techniques

Aux côtés d'un acteur dédié, le SGDN, d'autres acteurs publics interviennent dans le secteur de la SSI.

Au sein **du SGDN[1], la DCSSI[2]** est chargée d'organiser les travaux interministériels et de préparer les mesures que le Secrétaire général de la Défense nationale propose au Premier ministre; elle prépare les dossiers en vue des autorisations, agréments, cautions ou homologations, et en suit l'exécution; elle met en oeuvre les procédures d'évaluation et de certification; elle participe aux négociations internationales; elle assiste les services publics dans le domaine de la SSI (conseil, audit, veille et alerte sur les vulnérabilités et les attaques, réponse aux incidents); elle assure la formation des personnels qualifiés dans son centre de formation (CFSSI).

La DCSSI mène également des inspections dans les systèmes d'information des ministères. Aux dessus du CERTA[3], elle a mis en place un centre opérationnel de la sécurité des systèmes d'information (COSSI), activé en permanence et chargé d'assurer la coordination interministérielle des actions de prévention et de protection face aux attaques sur les systèmes d'information. Elle a également mis en place un nouveau label ainsi qu'une cellule chargée d'entretenir des relations avec le tissu des entreprises de SSI.

L'effectif de la DCSSI est d'une centaine de personnes, en majorité de formation scientifique et technique. Les auditions menées ont montré en particulier que :
– la faiblesse de l'effectif conduit à limiter la capacité d'inspection de la DCSSI à seulement une vingtaine de déplacements par an sur site, ce qui est insuffisant;
– son rôle de conseil aux entreprises est insuffisamment développé et se révèle peu en phase avec les attentes du monde économique;
– les formations du CFSSI[4], considérées comme de très grande qualité, sont malheureusement réservées aux personnels de l'administration exerçant directement dans le domaine de l'informatique ou de la SSI et souffrent d'un manque de notoriété.

Le ministère de la Défense est un acteur important pour les produits gouvernementaux de haut niveau de sécurité. Il est maître d'oeuvre des équipements ou moyens destinés à protéger les systèmes d'information gouvernementaux. Il a également la capacité d'apporter son concours aux contrôles et mesures que peuvent nécessiter les systèmes d'information en service dans les départements civils. Enfin, il est chargé de doter l'État des équipes et laboratoires de mesures propres à satisfaire l'ensemble des besoins gouvernementaux. En outre la Direction générale de la sécurité extérieure (DGSE), rattachée au ministère de la Défense, apporte sa connaissance des menaces étrangères sur les systèmes d'information. La Direction de la protection et de la sécurité de la défense (DPSD) assure de son côté une veille sur la sécurité des industries de défense.

Le ministère de l'Économie, des Finances et de l'Industrie a pour mission l'animation du développement industriel d'équipements de sécurité non-gouvernementaux. Le service des technologies et de la société de l'information (STSI) de la direction générale des entreprises (DGE) du ministère a un bureau du multimédia et de la sécurité qui suit le domaine SSI et finance des projets SSI au travers des appels à projets Oppidum. Enfin, comme pour les autres domaines technologiques, le MinEFI contribue au financement de l'innovation dans les PME par divers mécanismes d'aide, en particulier le crédit impôt-recherche, et au travers d'OSEO-ANVAR dont il assure la tutelle.
L'ADAE[5] assure la maîtrise d'ouvrage des services opérationnels d'interconnexion et de partage des ressources pour l'administration électronique, dont le volet sécurité regroupe toutes les activités nécessaires à la mise en place de l'infrastructure de confiance (outils, référentiels, guides méthodologiques et expertise). Alors que la SSI est une composante importante de ce type de projets, la DCSSI n'est pas citée dans le décret instituant l'ADAE.

1 Secrétariat général de la défense nationale.
2 Direction centrale de la sécurité des systèmes d'information.
3 Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques.
4 Centre de formation à la sécurité des systèmes d'information.
5 Agence pour le développement de l'administration électronique, rattachée au ministre chargé du Budget et de la réforme de l'État.

Le ministère de l'Intérieur est chargé de la lutte contre la cyber-criminalité. Dans le cadre de ses missions, la Direction de la surveillance du territoire (DST) assure des prestations techniques et informatiques autour de trois volets : la prévention, la répression et la sécurité informatique. L'OCLCTIC[6] est une structure à vocation interministérielle placée au sein de la Direction de la police judiciaire (DCPJ). Elle lutte contre les auteurs d'infractions liées aux TIC, enquête à la demande de l'autorité judiciaire, centralise et diffuse l'information sur les infractions à l'ensemble des services répressifs. La Police parisienne dispose d'un service similaire, le BEFTI.

La CNIL, en matière de sécurité des systèmes d'information, s'intéresse essentiellement à la protection des données personnelles. La loi du le 6 août 2004 lui donne une mission de labellisation de produits et de procédures. La CNIL a un pouvoir d'imposer que n'a pas la DCSSI. La CNIL et la DCSSI ont commencé à travailler ensemble.
La multiplication des acteurs publics, dont les missions se chevauchent et dont les textes fondateurs sont peu précis, donne une impression générale de confusion et d'éparpillement des moyens et des hommes. Dans cette nébuleuse, l'acteur public dédié, le SGDN et plus précisément la DCSSI, souffre d'un manque d'autorité et parfois de crédibilité auprès des publics concernés. Ces deux facteurs, l'éparpillement des moyens et le manque d'autorité du SGDN, nuisent à l'efficacité de l'État dans la définition et la mise en oeuvre de la politique globale de SSI.

De plus, les disparités dans la mise en oeuvre d'une organisation type, au sein de l'administration, des difficultés à mobiliser les ressources nécessaires et l'absence d'autorité des acteurs de la SSI, peuvent rendre cette organisation inopérante. Face aux difficultés de recrutement de personnels, des ministères sont conduits à recourir à l'externalisation. Il est fréquent de constater que les services informatiques ne suivent pas les recommandations des HFD[7] lors de choix de solutions pour des applications sensibles, sous couvert d'une stricte application du code des marchés publics. Toutefois certains ministères ont mieux intégré la problématique SSI et s'appuient sur des équipes compétentes et motivées.
Une analyse comparative de l'organisation, du budget consacré à la SSI, de l'existence de schémas directeurs opérationnels, de la classification des données sensibles et de la mise en place de chartes utilisateurs, effectuée dans cinq ministères, révèle une hétérogénéité pour chacun de ces domaines.

De plus, aucune politique « produits » globale n'existe dans le domaine de la SSI.

Le rapport analyse la situation de plusieurs pays (États-Unis, Royaume-Uni, Allemagne, Suède, Corée du Sud et Israël) et aborde les initiatives multilatérales (Union européenne, OCDE, ONU, G8, réseaux de veille et d'alerte). On ne retiendra dans cette synthèse que le cas de l'Allemagne.
L'Allemagne a adopté en juillet dernier un plan national pour la protection des infrastructures d'information (NPSI) qui s'appuie notamment sur l'homologue de la DCSSI, le BSI. Le BSI mène des actions de sensibilisation à destination des citoyens et des PME, analyse les tendances et les risques futurs ; il apporte une aide à la sécurisation des administrations mais aussi des entreprises (tenue à jour d'un standard professionnel de bonnes pratiques, conseils et support technique, tests d'intrusion, protection des infrastructures critiques); il analyse les risques, évalue et certifie des produits et donne l'autorisation des applications classifiées. Il participe au développement des produits et des technologies et joue un rôle actif dans les comités nationaux et internationaux de normalisation et de standardisation relatifs à la SSI.

Pour assurer l'ensemble de ces missions, le BSI emploie 430 personnes (contre 100 à la DCSSI) en croissance régulière depuis 2001. Il dispose d'un budget significatif de 51 millions d'euros en augmentation régulière depuis 2002. La part consacrée aux développements représente 19 % de ce budget (10 M€) et celle consacrée aux études 17 % (9 M€). Ces ressources sont sans commune mesure avec celles de la DCSSI.

6 Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.
7 Haut fonctionnaire de défense.

Le système d'information de l'entreprise est désormais déployé dans un contexte d'entreprise étendue permettant un travail en réseau avec ses clients ou usagers, ses fournisseurs, ses donneurs d'ordre, ses partenaires ou les représentants de l'administration. Ces interconnexions génèrent des vulnérabilités nouvelles pour les systèmes d'information de l'entreprise. En outre, la généralisation des outils nomades (téléphones mobiles, PDA, ordinateurs portables...) et le passage au tout numérique gomment la frontière entre espace professionnel et espace privé, accentuant très significativement les risques. Les enquêtes montrent que de nombreux sinistres ont été identifiés, avec des incidences considérables sur la production, l'équilibre financier ou l'image des entreprises. De plus, des actions d'espionnage industriel peuvent se traduire par une perte de compétitivité avec une incidence négative sur l'emploi.

Cependant, sécuriser les systèmes d'information requiert de mobiliser des ressources financières et humaines dont le retour sur investissement est souvent difficile à justifier. Les PME ont notamment du mal,du fait de leur faible taille, à disposer des ressources nécessaires.

Si l'intégration de la SSI dans le modèle culturel de l'entreprise reste une exception, certaines grandes entreprises internationalisées montrent une maîtrise remarquable de la SSI : politique de sécurité imposée au plus au haut niveau, organisation efficace, sensibilisation et responsabilisation des personnels, choix d'architectures et d'équipements adaptés à la sécurisation des informations stratégiques, etc.

Les entreprises attendent de l'État des services de support efficaces et accessibles, comme un guichet unique pour les aider à résoudre leurs problèmes de SSI, des préconisations de produits de sécurité, un soutien spécifique lorsqu'elles sortent des frontières, etc. Divers organismes publics et privés ont élaboré à l'attention des entreprises d'excellents guides.

Base industrielle et technologique

Les États-Unis disposent d'une domination sans partage sur la plupart des segments du marché de la SSI. Pourtant, la sécurité des systèmes d'information est un enjeu national à caractère stratégique, politique et économique. Dans une logique de souveraineté, la France et l'Europe peuvent-elles aujourd'hui se doter des moyens d'assurer de manière autonome la protection de leurs infrastructures et de leurs systèmes ?

Les technologies de sécurité sont à la base du développement des produits et conditionnent ainsi directement la qualité de la SSI. La conception d'architectures de sécurité, l'ingénierie logicielle, la preuve de programmes et de protocoles et les méthodes d'évaluation, la cryptographie, les dispositifs électroniques de protection de secrets (cartes à puces...) et les méthodes applicatives de filtrage (antispam, antivirus...), de modélisation du comportement et de détection d'intrusions, sont globalement bien maîtrisées au niveau national contrairement aux systèmes d'exploitation et aux circuits intégrés sécurisés, technologies pourtant essentielles à la sécurité de la plupart des équipements. C'est sur elles que devrait porter un effort massif de recherche et de développement.

Quelques centres et instituts en France ont des activités orientées SSI, en logiciels ou matériels, pour certains de grande réputation. Toutefois l'absence de grands leaders industriels en France, une insuffisance de fonds publics dédiés et la contrainte des publications ne permettent pas à la recherche nationale en SSI d'être au niveau des meilleurs mondiaux.

Une coopération accrue avec des leaders étrangers présenterait des risques mais permettrait, dans le cadre de partenariats réellement équilibrés, de mettre les chercheurs français au contact de ces leaders.

Le marché de la SSI est en forte croissance mais reste de faible volume.

Le tissu industriel national en SSI est constitué de quelques grands groupes, souvent liés au marché de l'armement, d'intégrateurs, de nombreuses SSII de toutes tailles, d'une centaine de petites et moyennes entreprises, souvent à forte valeur technologique, qui peinent pour la plupart à survivre, et de leaders mondiaux dans le domaine de la carte à microprocesseurs. Cependant, l'offre nationale et européenne est éclatée. *Des actions visant au rapprochement de ces activités, en s'inspirant de ce qui a été fait dans la Défense et l'Aéronautique, deviennent impératives.*

Les politiques d'achat de l'État et des grands donneurs d'ordres ne sont pas favorables aux PME innovantes. À l'exception du pacte PME proposé par le Comité Richelieu en association avec OSEO-Anvar, il n'y a pas de réelle dynamique de la part des grands donneurs d'ordres.

Les PME de la SSI ne disposent pas des ressources suffisantes pour affronter la concurrence des offres étrangères. Elles ont des difficultés à financer leurs investissements, que ce soit en fonds propres (le secteur n'attire pas les investisseurs nationaux) ou par des crédits bancaires. Il faudrait développer des fonds d'investissement spécifiques, adaptés à des entreprises de croissance modérée, à même d'assurer un financement stable sur une durée supérieure à 10 ans.

Le financement public de la R&D est insuffisant dans les TIC en général. Si différentes sources de financement existent, plus ou mois accessibles aux PME : l'Anvar, l'ANR (Agence nationale de la recherche), l'A2I (Agence de l'innovation industrielle), les ministères chargés de l'Industrie et de la Recherche et l'Union européenne, ces financements sont insuffisants et mal coordonnés.

Enfin, si l'environnement juridique et fiscal des entrepreneurs est en amélioration, il demeure perfectible.

Labellisation des produits de sécurité. La France fait partie des pays fondateurs des critères communs et des accords de reconnaissance mutuelle. Il est toutefois regrettable de constater que sa compétence
et son expérience particulière (en particulier de ses centres d'évaluation) sont trop peu connues et reconnues à l'étranger.
– Une évaluation est conduite par un laboratoire privé, CESTI, agréé par la DCSSI.
– Le processus de certification est jugé trop long et trop coûteux par beaucoup d'industriels, a fortiori pour les PME.
– La qualification par la DCSSI est donnée à un produit qui a été évalué et certifié à partir d'une « cible de sécurité » qu'elle a approuvée au préalable. 10 produits ont déjà été qualifiés et 7 sont en cours de qualification. La moitié de ces produits est développée par des PME...
– L'agrément est l'attestation délivrée par la DCSSI qu'un produit de chiffrement est apte à protéger des informations classifiées de défense, après évaluation par le Celar et par la DCSSI. C'est un label national.

La normalisation facilite les choix stratégiques de l'entreprise, favorise la protection des consommateurs et l'application de la réglementation. La présence de la France dans la normalisation et la standardisation est notoirement insuffisante.
Une des voies pour faciliter l'acquisition des produits qualifiés est de donner à des profils de protection le statut de normes françaises homologuées. Le projet de convention entre la DCSSI et l'AFNOR pour mener à terme une action de normalisation est toujours en discussion. Il y faudrait une nouvelle impulsion.

Document 5

Les entreprises face au défi de la sécurité informatique
Par Caroline De Malet
Mis à jour le 10/03/2014 à 11:40
Publié le 09/03/2014 à 17:09

Le CeBIT, salon du high-tech, a été inauguré dimanche par Angela Merkel et David Cameron.

Pas moins de deux chefs d'État pour inaugurer le CeBIT, le grand salon consacré au high-tech, avec 200.000 visiteurs attendus: Angela Merkel et David Cameron se sont ainsi retrouvés dimanche soir à Hanovre pour donner le coup d'envoi de cette rencontre sur laquelle plane l'ombre de l'affaire de la NSA.

Dans le cadre de ce salon, désormais réservé exclusivement aux professionnels, les débats devraient réserver une large place à la sécurité informatique.

Il faut dire que la fréquence des cyber-attaques aurait doublé l'an dernier, selon l'entreprise de sécurité informatique américaine FireEye: leur rythme serait passé de une toutes les trois secondes en 2012 à une toutes les 1,5 seconde en 2013.

73 % des directions informatiques mondiales interrogées par le cabinet britannique Vanson Bourne pour Dell affirment ainsi avoir déjà été l'objet d'une faille de sécurité depuis un an. 17 % en moyenne du budget d'une direction informatique est dédié à la sécurité et 74 % d'entre elles prévoient d'augmenter celles-ci au cours des deux ou trois années à venir.

Les PME sont les plus vulnérables

Mais à en croire une étude de la SSII Steria sur la sécurité en Europe, 60 % des décideurs informatiques considèrent que le vol de données est le risque le plus important encouru, tandis que 37 % d'entre eux redoutent l'espionnage. « Les APT (advanced persistent threat), la menace en trois lettres qui devrait faire trembler les responsables sécurité, ne sont en revanche pas identifiés parmi les risques majeurs », souligne l'étude.

> « La tendance aujourd'hui est au cloud hybride, qui profite de la puissance de stockage des données externalisées et conserve en interne uniquement les données les plus sensibles »
>
> Marc Montiel, vice-président de la région Europe du Sud de NettApp

Par ailleurs, seuls 46 % des directeurs informatiques interrogés déclarent utiliser des dispositifs de sécurité dans le cloud, alors que 73 % hébergent leurs données dans le nuage. « Après l'apparition du cloud public, sous-traité à un prestataire extérieur, les entreprises ont préféré réintégrer leurs données dans des clouds privés gérés en interne. La tendance aujourd'hui est au cloud hybride, qui profite de la puissance de stockage des données externalisées et conserve en interne uniquement les données les plus sensibles », explique Marc Montiel, vice-président de la région Europe du Sud de NettApp. En revanche, les clouds souverains - Numergy et Cloudwatt en France - qui hébergent les données sur le territoire national précisément pour des raisons de sécurité, ont du mal à décoller, Cloudwatt démarrant seulement la commercialisation de ses offres.

À noter qu'il existe de grandes disparités : « En Grande-Bretagne, la culture de l'externalisation est très développée, alors qu'en France on externalise la sécurité avant tout pour réduire ses coûts », fait remarquer Florent Skrabacz, directeur des activités sécurité de Steria.

Paradoxe: les entreprises les moins prêtes à investir pour se protéger sont les PME, précisément les plus vulnérables. Car les cyberpirates savent que la plupart d'entre elles sont la clé d'entrée vers les grandes sociétés dont elles sont les sous-traitants. Le marché reste donc porteur.

Document 6

Cyberdéfense : un nouvel enjeu de sécurité nationale

Sénat, Rapport d'information n° 449 (2007-2008) de M. Roger ROMANI, fait au nom de la commission des affaires étrangères, déposé le 8 juillet 2008.

Les attaques informatiques s'affranchissent des frontières et peuvent être dirigées simultanément contre plusieurs États. La surveillance des réseaux et la mise au point des réactions en cas d'incident justifie une coopération et une assistance internationales. De manière plus générale, la protection des systèmes d'information face aux activités illégales constitue aujourd'hui une préoccupation commune à de nombreux États.

Plusieurs organisations multilatérales ont mis la sécurité des systèmes d'information à l'ordre du jour de leurs travaux.

L'ONU a adopté plusieurs documents concernant les technologies de l'information et de la communication et leurs aspects relatifs à la sécurité.

L'Union internationale des télécommunications (UIT) a organisé, en liaison avec l'Assemblée générale des Nations unies et sur deux sessions qui se sont déroulées en 2003 et 2005, le sommet mondial sur la société de l'information, au cours duquel a été abordée la question de la gouvernance de l'internet. L'UIT travaille à l'établissement d'un cadre international pour la promotion de la cybersécurité (Programme mondial cybersécurité*)* et vient de créer un groupe d'experts de haut niveau chargé de proposer une stratégie à long terme englobant les mesures légales, les mesures techniques visant à remédier aux failles des produits logiciels, ainsi que la prévention et la détection des attaques informatiques et la gestion de crise,

L'OCDE et le G8 mènent également des travaux sur le sujet.

Votre rapporteur évoquera plus précisément les coopérations opérationnelles entre structures d'alerte et d'assistance, ainsi que les actions menées dans le cadre de l'OTAN et de l'Union européenne.

1. La coopération opérationnelle des structures d'alerte et d'assistance (CERT)

Comme on l'a précédemment indiqué, un très grand nombre de pays ont mis en place des CERT (*Computer emergency response team*), structures permanentes d'alerte et d'assistance chargées d'assurer, pour le compte des organismes qui s'y sont rattachés (administrations, centres de recherche, entreprises), une double mission d'information sur les vulnérabilités, les menaces en cours et les moyens d'y parer, et d'assistance en vue de résoudre les incidents.

Dès 1990, l'utilité de procéder à des **échanges entre les différents CERT** a été reconnue, avec la création d'une **enceinte internationale**, le *Forum of incident response and security teams* (**FIRST**).

Le FIRST a pour buts de favoriser la coopération entre les équipes pour prévenir, détecter et rétablir un fonctionnement nominal en cas d'incident de sécurité informatique, de fournir un moyen de communication commun pour la diffusion de bulletins et d'alertes sur des failles potentielles et les incidents en cours, d'aider au développement des activités de ses membres en matière de recherche et d'activités opérationnelles, et de faciliter le partage des informations relatives à la sécurité, des outils, des méthodes et des techniques. Il organise une conférence annuelle internationale consacrée au traitement des incidents de sécurité et aux échanges d'expérience et d'expertise dans ces domaines.

Aujourd'hui, **le FIRST fédère près de 200 CERT répartis de par le monde**.

Une **enceinte spécifique,** l'**EGC** (*European Government Computer Security Incident Response Teams*), a été créée par **certains pays européens** pour regrouper leurs structures gouvernementales. Le CERTA, CERT gouvernemental français, y participe avec ses homologues allemand, britannique, néerlandais, suisse, suédois, finlandais et norvégien.

L'EGC a pour but d'encourager le développement conjoint des mesures pour résoudre des incidents de sécurité de grande ampleur et de faciliter le partage d'informations et les échanges technologiques concernant les incidents de sécurité informatique, les menaces liées à des codes malveillants ainsi que les vulnérabilités des systèmes d'informations. L'EGC s'efforce également d'identifier des domaines de compétences spécialisés et d'expertise qui peuvent être partagées au sein du groupe, ainsi que des projets de coopération en matière de recherche et développement.

D'après les indications de l'Agence européenne de la sécurité des réseaux et de l'information (ENISA), seuls huit pays membres de l'Union européenne disposaient d'un CERT gouvernemental en 2005. Leur nombre s'élève à 14 actuellement et la quasi-totalité des pays membres devraient être dotés d'un CERT gouvernemental d'ici un à deux ans.

2. Une nouvelle priorité de l'OTAN

Le thème de la cyberdéfense a retenu l'attention de l'OTAN dès le sommet de Prague, en 2002, dont la déclaration finale préconisait un renforcement des capacités de l'Alliance contre les attaques informatiques.

L'OTAN s'est préoccupée dans un premier temps de la protection de ses propres systèmes d'information et de communication, et elle a mis en place à cet effet une structure spécifique (*Nato computer incident response capability - NCIRC*).

Les évènements survenus en Estonie au printemps 2007 ont amené l'OTAN à s'interroger sur son rôle, en tant qu'alliance défensive, en cas d'attaque contre l'un de ses membres.

Les réflexions menées depuis lors ont abouti à l'élaboration d'un **concept de cyberdéfense de l'OTAN** qui a été approuvé en début d'année 2008. Lors du sommet de Bucarest, au mois d'avril dernier, les chefs d'Etat et de gouvernement de l'Alliance ont souligné « *la nécessité pour l'OTAN et pour les pays de protéger les systèmes d'information clés conformément à leurs responsabilités respectives, de mettre en commun les meilleures pratiques, et de mettre en place une capacité visant à aider, sur demande, les pays de l'Alliance à contrer les cyberattaques* ».

Cette politique de cyberdéfense vise tout d'abord à **renforcer la sécurité des systèmes d'information de l'Alliance**, grâce à l'amélioration des normes et des procédures de sécurité, et à une gestion plus centralisée.

Elle a également pour objectif de **renforcer la capacité de l'OTAN à coordonner l'assistance aux alliés subissant une attaque informatique d'importance, le cas échéant à l'aide d'équipes projetables**.

Le partage des responsabilités entre l'OTAN et les nations, qui conservent la charge de la protection de leurs propres systèmes d'information, a été défini de manière à bien délimiter le périmètre des systèmes à partager.

L'OTAN prévoit de créer une **autorité chargée de la cyberdéfense** (*NATO Cyber Defense Management Authority - CDMA*) qui constituera le point central pour la coordination de la politique de l'Alliance et l'analyse des besoins, en regroupant l'ensemble des compétences en la matière.

Par ailleurs, huit pays alliés[3(*)] ont décidé de contribuer à la création d'un **centre d'excellence sur la cyberdéfense** rattaché à l'OTAN. Constitué à partir d'une capacité estonienne déjà existante, ce centre situé à Tallin et inauguré à la fin du mois de mai dernier est constitué d'une trentaine d'experts provenant des pays impliqués. Ce centre n'a pas de vocation opérationnelle. Son objectif est de réunir au profit de l'Alliance l'expertise en matière de risques cybernétique, d'élaboration d'une doctrine, de retour d'expérience et de formation d'experts.

Il faut noter que la France a largement participé au processus de définition de la politique de cyberdéfense de l'OTAN qui, en moins d'un an, aura permis de définir un concept global et de le décliner en une organisation cohérente.

3. L'action encore lacunaire de l'Union européenne

Les instances européennes ont adopté de **nombreux documents d'orientation et programmes** intéressant directement ou indirectement la sécurité des systèmes d'information. Pour la période récente, on peut citer : la stratégie dite « i2010 » (« Une société de l'information pour la croissance et l'emploi ») exposée dans une communication de la Commission européenne du 1er juin 2005, et qui confirme l'importance de la sécurité des réseaux ; la communication de la Commission du 31 mai 2006, intitulée « Une stratégie pour une société de l'information sûre - dialogue, partenariat et responsabilisation », qui propose notamment une évaluation comparative des politiques nationales relatives à la sécurité des réseaux et de l'information ; la communication de la Commission du 12 décembre 2006 sur un programme européen de protection des infrastructures critiques qui préconise une approche européenne commune de la sécurité de ces infrastructures et inclura nécessairement les préoccupations liées aux systèmes d'information.

On peut observer que ces documents fixent des objectifs très généraux, mais ne paraissent pas encore en mesure de se traduire rapidement par des initiatives concrètes.

L'Union européenne dispose cependant d'un instrument spécialisé à travers l'Agence européenne chargée de la sécurité des réseaux et de l'information, l'**ENISA** (*European Network and Information Security Agency*), créée en 2004 avec un mandat initial d'une durée de cinq ans.

Installée à Heraklion, en Crète, **l'ENISA s'est vue assigner des missions très vastes** : conseiller et assister la Commission et les États membres en matière de sécurité de l'information et les aider, en concertation avec le secteur, à faire face aux problèmes de sécurité matérielle et logicielle ; recueillir et analyser les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents ; promouvoir des méthodes d'évaluation et de gestion des risques afin d'améliorer notre capacité de faire face aux menaces pesant sur la sécurité de l'information; favoriser l'échange de bonnes pratiques en matière de sensibilisation et de coopération avec les différents acteurs du domaine de la sécurité de l'information, notamment en créant des partenariats entre le secteur public et le secteur privé avec des entreprises spécialisées; suivre l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information.

L'ENISA a fait l'objet d'une **évaluation externe** demandée par la Commission qui en a publié le résultat en juin 2007. Le groupe d'experts externe a conclu que **les activités de l'ENISA paraissaient «** *insuffisantes pour atteindre le niveau élevé d'impact et de valeur ajouté espéré* **»** et que sa visibilité était en dessous des attentes. L'évaluation recense divers handicaps liés à son organisation, aux ambiguïtés du mandat originel, à sa localisation éloignée, à l'effectif et à la rotation importante du personnel, aux relations difficiles entre le conseil d'administration et la direction de l'agence. Elle souligne un risque d'affaiblissement rapide et de perte de réputation si l'efficacité n'était pas améliorée.

Une proposition de règlement prévoit la prolongation à l'identique du mandat de l'ENISA jusqu'en 2011, date à laquelle son avenir devrait être réexaminé.

Cette perspective de réorganisation témoigne des **interrogations qui subsistent sur les missions et l'action de l'ENISA** au service des objectifs poursuivis par l'Union européenne.

Le Livre blanc sur la défense et la sécurité nationale rendu public le 17 juin dernier souligne à cet égard que « *l'efficacité de l'agence européenne ENISA devra également être très notablement accrue* », notamment pour permettre à la Commission européenne de mettre en place un volet « sécurité des systèmes d'information » dans toutes les réalisations des institutions européennes.

Par ailleurs, le Livre blanc juge **indispensable de renforcer la coopération opérationnelle** au sein de l'Union européenne, afin qu'elle soit la plus réactive possible entre Etats membres face aux attaques contre les systèmes d'information.

La France proposera également que la **Commission impose aux opérateurs des règles de durcissement des réseaux et des procédures** destinées à en accroître très fortement la résilience.

** [3] Allemagne, Espagne, Estonie, Finlande, Italie, Lettonie, Lituanie et Slovaquie.*

Document 7

Une attaque informatique de portée mondiale crée la panique

Des hôpitaux britanniques et des entreprises espagnoles ont été touchés par des virus, vendredi. Ils bloquent l'accès aux fichiers d'un ordinateur afin d'obtenir une rançon.

LE MONDE | 12.05.2017 à 18h43 • Mis à jour le 19.05.2017 à 16h38

Les autorités américaines ont mis en garde vendredi 12 mai contre une vague de cyberattaques simultanées qui a touché des dizaines de pays dans le monde, recommandant de ne pas payer de rançon aux pirates informatiques. Ceux-ci ont apparemment exploité une faille dans les systèmes Windows, divulguée dans des documents piratés de l'agence de sécurité américaine NSA.

« Nous avons reçu de multiples rapports d'infection par un logiciel de rançon, a écrit le ministère américain de la sécurité intérieure dans un communiqué. *Particuliers et organisations sont encouragés à ne pas payer la rançon car cela ne garantit pas que l'accès aux données sera restauré. »*

Cette vague d'attaques informatiques de *« portée mondiale »* suscite l'inquiétude des experts en sécurité. Le virus en cause est un *ransomware* (« rançongiciel »), un programme qui bloque l'accès aux fichiers d'un ordinateur en vue d'obtenir une rançon.

« Nous avons relevé plus de 75 000 attaques dans 99 pays », a noté Jakub Kroustek, de la firme de sécurité informatique Avast, sur un blog. Forcepoint Security Labs, autre entreprise de sécurité informatique, évoque de son côté *« une campagne majeure de diffusion d'emails infectés »*, avec quelque 5 millions d'emails envoyés chaque heure répandant le logiciel malveillant appelé WCry, WannaCry, WanaCrypt0r, WannaCrypt ou Wana Decrypt0r.

« Si la NSA avait discuté en privé de cette faille utilisée pour attaquer des hôpitaux quand ils l'ont "*découverte*"*, plutôt que quand elle leur a été volée, ça aurait pu être évité »*, a regretté sur Twitter Edward Snowden, l'ancien consultant de l'agence de sécurité américaine qui avait dévoilé l'ampleur de la surveillance de la NSA en 2013.

300 dollars de rançon

Ces attaques informatiques ont notamment touché le service public de santé britannique, comme l'a dénoncé la première ministre britannique, Theresa May, lors d'une intervention télévisée. L'attaque a visé simultanément seize entités dépendant du *National Health Service* (NHS – la Sécurité sociale britannique), a écrit l'organisme dans un communiqué. L'utilisation de leurs ordinateurs a été perturbée, les obligeant à refuser des patients en urgence.

Selon le NHS, le logiciel en cause pourrait être une variante de Wanna Decryptor, tout en avertissant que l'enquête technique débutait tout juste. *« A ce stade de l'enquête, nous ne disposons pas de preuve que les données de patients ont été compromises »*, écrit également le NHS. *« Nous avons activé le Centre national de cybersécurité et ils travaillent avec les organisations du NHS touchées pour s'assurer qu'elles sont aidées et que la sécurité des patients est garantie »*, a ajouté Theresa May.

Le logiciel demande 300 dollars en l'échange du déchiffrement des fichiers. Un journaliste britannique spécialisé a partagé sur Twitter le message s'affichant sur les ordinateurs touchés. *« Oups, vos fichiers ont été chiffrés »,* peut-on y lire à côté de deux comptes à rebours décomptant le temps restant avant la *« perte »*, faute de paiement, des fichiers chiffrés.

Un des groupements d'hôpitaux touché a annoncé *« repousser toutes les activités non urgentes »*. En 2016, quatre hôpitaux britanniques avaient déjà été paralysés durant plusieurs jours par des rançongiciels.

Des cas similaires dans le monde entier

« Cela ne vise pas le NHS, c'est une attaque internationale et plusieurs pays et organisations ont été touchés », a déclaré la première ministre Theresa May. Cette vague de rançongiciels semble en effet dépasser les seuls hôpitaux britanniques. Des organisations en Espagne, en Australie, en Belgique, en France, en Allemagne, en Italie et au Mexique ont également été touchées selon des analystes. Aux Etats-Unis, le géant de livraison de colis FedEx a reconnu avoir lui aussi été infecté. Le ministère de l'intérieur russe a également annoncé avoir été touché par un virus informatique vendredi, même s'il n'a pas été précisé s'il s'agit bien de la même attaque.

Par ailleurs, un chercheur de l'entreprise de sécurité informatique Avaast dit que sa société a détecté cette après-midi un très grand nombre de virus identiques dans le monde entier, principalement en Russie, en Ukraine et à Taïwan. Selon l'entreprise spécialisée en sécurité informatique, au moins 45 000 tentatives d'infections ont été repérées dans environ 74 pays.

Selon le quotidien espagnol *El Mundo*, environ 85 % des ordinateurs appartenant à Telefonica ont été touchés par ce virus, qui demande ici une rançon en bitcoins (célèbre monnaie dématérialisée) équivalant à 300 dollars. Certains employés ont été renvoyés chez eux, étant dans l'incapacité de travailler.

Le Centre cryptologique national (CCN) – division des services de renseignements chargée de la sécurité informatique – a évoqué l'implication d'un virus connu sous le nom WannaCry. D'autres entreprises espagnoles, comme Iberdrola et Gas Natural, ont demandé à certains de leurs employés d'éteindre leurs ordinateurs, explique *El Mundo*, sans déterminer s'il s'agissait de mesures préventives ou du résultat d'une attaque

Insee
Mesurer pour comprendre
Direction générale

CONCOURS DE CONTRÔLEUR DE L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES

ANNÉE 2019

ÉPREUVE FACULTATIVE D'ALLEMAND

Aucun dictionnaire ou dispositif d'aide à la traduction n'est autorisé

Janvier 2019
(durée 1 heure 30 - coefficient 1)
Le sujet comporte 3 pages

1. Übersetzen Sie den Textteil 4. (10 Punkte)

2. Erklären Sie folgende im Text unterstrichene Wörter auf Deutsch. (2,5 Punkte)

a) stattdessen

b) Herangehensweise

c) wachsenden

d) Vorgesetzter

e) Bedarfsanalyse

3. Beantworten Sie folgende Fragen auf Deutsch:

a) Welche Konsequenzen hat es für den Bildungssektor, dass China für deutsche Unternehmen immer wichtiger wird? (ca. 50 Wörter / 2,5 Punkte)

b) Was bedeutet „interkulturelle Kommunikation“ und warum ist sie in unserer heutigen Welt wichtig? Begründen Sie Ihre Position und geben Sie praktische Beispiele. (ca. 150 Wörter / 5 Punkte)

Ni hao

Wie verhandeln Chinesen? Und was muss bei Mails an Südamerikaner beachtet werden? Interkulturelle Kompetenz kann man lernen, berichtet Lara Sogorski.

1 WENN DEUTSCHE verhandeln, erwarten sie klare Aussagen von ihren Gegenuber: Ja oder Nein? Da kann es sehr irritieren, wenn sie stattdessen nur ein unbestunmtes „Wirwerden-sehen" zu hüren bekommen. Produktrnanagerin Diana Ide-Hehr, in einer Firma, die unter anderem in China produzien. für das internationale Geschaft zustandig, war schon oft in einer solchen schwierigen Situation. Wahrend sie es gewohnt ist, Entscheidungen kurz und knapp zu treffen, stügt sie damit bei ihren chinesischen Geschaftspannern auf hoflichen Widerstand. „Ich erlebe in meinem beruflichen Alltag, in Gesprachen mit chinesischen Partnern, immer wieder, dass sie eine ganz andere Herangehensweise an Verhandlungen haben ais wir Deutschen", sagt die 36-Jahrige. „Wir Deutschen sind sehr direkt, doch die Chinesen dracken sich bei einer Entscheidung zum Beispiel gern cher vage aus. Und ich habe mich gefragt, warum ticken die so?"

2 Inzwischen weil die Produktmanagerin mehr über die talitat, die Kultur und die Geschichte der Chinesen und sie hat sogar erwas Chinesisch gelernt. Bei der Fernhochschule AKAD entdeckte sie im vergangenen Jahr die Weiterbildung „Interkulturelie Kommunikation China" und meldete sich sofort an. „Ich hat-te schon langer nach einer ivInglichkeit gesucht, etwas über China, das Land, die Kultur und Menschen zu lernen. Aber auch die Sprache und die Zeichen wolite ich verstehen." Zumindest auf einem Basisniveau.

3 Wie Diane Ide-Herh arbeiten heute viele Menschen in interkul-rurellen Teams tuici liber die deut-schen Landesgrenzen hinaus. Dabei kann es jedoch schnell zu Schwierigkeiten kommen, denn eine untetschiedliche Kultur be-deutet klare Unterschiede und auch Missverstandnisse. Hier ist interkulturelle Kompetenz ge-fragt, also das Wissen, wie die an-dere Kultur so rickt und warum. Entsprechende Weiterbildungen und Seminare hieten mittlerweile eine ganze Reihe von Unterneh-men und Einrichtungen an - im-mer haufiger mit dem Fokus auf China.

4 „China wird für deutsche Unternehmen immer wichtiger, daher verbringen immer mehr Arbeitnehmer betriehlich bedingt einige Zeit in China, zum Teil auch mit ihren Familien. Das führt zu einer stetig wachsenden Nachfrage nach Chinesischunterricht und vorbereitenden interkulturellen Kursen", heilit es beim Anbieter AKAD. Der Lehrgang sei in seiner The menzusammenstellung daher so konzipiert, dass er ouf einen solchen Aufenthalt vorbereite. Das hei&, die Teilnehmer sollen am Ende die kulturell bedingten Hintergründe des Verhaltens von Chinesen verstehen und sich auf dem Sprachniveau A1/A2 mit ihnen unterhalten künnen.

5 Der Kurs ist zwar vor allem theoretisch aufgebaut, mit Texten und Online-Übungen, aber: ..Die Teilnehrner belegen ja den Kurs nicht im luftleeren Raum, sondern meist mit konkretem Bezug zu ihren beruflichen oder privaten Aktivitaten in Sachen China", heigt es bei AKAD. So sei es für die Zielgruppe müglich, sich das in der Praxis bendtigte Hintergrundwissen flexibel an-zueignen.

6 So war es auch bei Diana Ide-Hehr. Sie haste durch ihren Beruf stets die praktische Erfahrung und konnte sich durch die Weiterbildung die nritige Theorie dazu holen. „Jetzt mit dem Wissen aus der Weiterbildung verstehe ich die Hintergründe und kann das Verhalten meines Gegenübers viel besser einordnen. Das er-leichtert meine Arbeit enorm." Jetzt kenne sie zum Beispiel die Hierarchieordnung der Chine-sen und wisse, an wen sie sich wenden musse, wenn sie eine bestimmte Frage habe. Wenn sie bei einem Ansprechpartner nicht weiterkommt, wendet sie sich jetzt an dessen Vorgesetzten, denn sie weiß jetzt: „Es gibt klare Kompetenzgrenzen und niemand von den Chinesen fühlt sich über-gangen, wenn man sich an den nachsthdheren Mitarbeiter wen-det." (...)

7 Ein ganz individuelles Training auch in Gruppen bietet das Unternehmen Intercultures in Berlin. Feste Kurse und Seminare gibt es hier nicht. Wer sich für eine andere Kultur interessiert, kann sich für ein offertes Training anmelden. Dabei steht am Anfang immer eine Bedarfsanalyse sodass die Inhalte nachher auch genau zu den Bedürfnissen der Teilnehmer passen. (...) „Unser Ziel ist es, dass jeder Teilnehmer am Ende das Werkzeug in der Hand hat, um Im Alltag im interkulturellen Kentext zurecht zu kommen", beschreibt Andrea Mendieta von Intercultures. Von Afrika über Asien, Lateinamerika, Amerkia bis hin zu Europa: Je nach Kontinent gibt es außerdem Experren für die einzelnen Landen Die Praxis mit Übungen und Rollenspielen steht hier im Vordergrund. So lernen die Teilnehmer eines Lateinamerika-Trainings zum Beispiel, wie sie eine geschaftliche E-Mail kultursensibel formulieren mtissen. (…)

Insee
Mesurer pour comprendre
Direction générale

CONCOURS DE CONTRÔLEUR DE L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES

ANNÉE 2019

ÉPREUVE FACULTATIVE D'ANGLAIS

Aucun dictionnaire ou dispositif d'aide à la traduction n'est autorisé

Janvier 2019
(durée 1 heure 30 - coefficient 1)
Le sujet comporte 4 pages

CTANGL191

After carefully reading the document, answer the following questions.

Please use your own words without quoting the text.

1/In the text, what is the key issue in the Brexit talks? What are the positions of political leaders on the situation? (4 points)

2/ Explain the different ways of creating an Irish backstop. Why is it called a “safety net” in the text? (3 points)

3/ Why is May under pressure from a domestic perspective? (3 points)

4/ According to you, what may be the consequences of a “soft Brexit" or a “hard Brexit” in the United Kingdom and in Europe? (10 points)

Brexit negotiations have hit a "real problem" over the issue of the Irish border, government sources have warned.

Ahead of a key summit, the EU is believed to be seeking further reassurances to prevent a so-called hard border involving physical checks. Hopes of a breakthrough were raised when the Brexit secretary made an unscheduled trip to Brussels on Sunday.

But talks faltered over the need for a back-up plan - known as the backstop - to avoid a hard border. UK Prime Minister Theresa May, who will make a statement later to MPs, has insisted any backstop arrangement should apply to the UK as a whole to avoid creating a new border in the Irish Sea.

But Sunday's talks had broken down after the EU had insisted on a second backstop arrangement - just involving Northern Ireland - if the UK's version wasn't ready in time, Downing Street sources indicated.

The Democratic Unionist Party has vowed to oppose any new checks on goods passing between Great Britain and Northern Ireland. And the party's Brexit spokesman has said the prospect of a no-deal Brexit is "probably inevitable". Ireland's Foreign Minister, Simon Coveney, suggested a deal would not be done at this week's summit, which starts on Wednesday.

Mr Coveney said he was "frustrated and disappointed" that it was going to take "more time than people had hoped". Scotland's First Minister Nicola Sturgeon, meanwhile, has set out her alternative Brexit plans, saying it is "time to compromise".

What is the Irish 'backstop'?

The UK is leaving the EU in March 2019, along with its single market and customs union, which allow for friction-free trade between members.

After Brexit, it will have a land border with the EU between Northern Ireland and the Republic. Both the UK and the EU want to avoid a "hard border" - physical checks or infrastructure between Northern Ireland and Ireland - but cannot agree how.

So, the backstop is a position of last resort - to protect an open border on the island of Ireland in the event that the UK leaves the EU without having agreed a solution as part of trade negotiations. The two sides do not agree on what this safety net should look like, however. The EU has suggested Northern Ireland stays aligned with its trade rules so new border checks are not needed. But Mrs May has said this would undermine the integrity of the UK by creating a new border in the Irish Sea.

She has suggested the UK as a whole could remain aligned with the EU customs union for a limited time after 2020, when the planned transition period ends.

But the EU says a backstop would not work if it is time-limited.

Some Tory Brexiteers say the backstop is not necessary at all because technological solutions can avoid a hard border.

Domestic pressure on May

This week's summit comes as domestic political pressure on Mrs May increases amid threats of potential cabinet resignations. Some Brexiteers are unhappy at the idea of the UK staying aligned to EU rules without a time limit being specified. At the weekend, former Brexit Secretary David Davis urged ministers to "exert their collective authority" and rebel against the plans.

But International Development Secretary Penny Mordaunt said she wasn't going to resign over the prime minister's Brexit plan.

"Everyone needs to calm down. We're entering the final stages of these negotiations and we're all behind the PM trying to get the best result," she added.

Arriving at an EU meeting in Luxembourg, Foreign Secretary Jeremy Hunt said the Brexit talks had entered a "difficult period", adding: "Whether a deal is done this week or not who knows?" He insisted it was possible to do a deal and "with goodwill on all sides we can get there".

But his predecessor, Boris Johnson, said the backstop plan should be scrapped altogether, saying the EU was trying to change the UK's constitutional arrangements and "treating us with naked contempt".

Sinn Fein leader Mary Lou McDonald told BBC Radio 4's Today programme: "It would be a chronic miscalculation and an utter disgrace if the policy of the British government was to be set by the most extreme elements of the Brexiteers and the needs and desires and the idiosyncrasies of the Democratic Unionist Party."

Labour, meanwhile, has called on the government to publish its plan for the backstop.

Shadow Brexit secretary Sir Keir Starmer said any proposal needed full scrutiny from MPs before an agreement could be struck with the rest of the EU at the Brussels summit.

A Number 10 source said the prime minister had made sure Parliament was regularly updated on the talks.

www.bbcnews.com , October 15 2018

Insee
Mesurer pour comprendre
Direction générale

CONCOURS DE CONTRÔLEUR DE L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES

ANNÉE 2019

ÉPREUVE FACULTATIVE D'ESPAGNOL

Aucun dictionnaire ou dispositif d'aide à la traduction n'est autorisé

Janvier 2019
(durée 1 heure 30 - coefficient 1)
Le sujet comporte 3 pages

Preguntas:

Lea muy atentamente el texto sacado de la prensa española. (20 minutos) Conteste las siguientes preguntas empleando su propio lenguaje (o sea evitando “copiar-pegar”)

1°) Apoyándose en el artículo, explique rápidamente de qué acontecimiento se trata. (10 minutos- 4 a 5 líneas- 3 puntos)

2°) Trate usted de explicar en qué puede tener un impacto para España semejante evento. ¿A nivel nacional? ¿A nivel internacional? (10 minutos- 4 a 5 líneas- 3 puntos)

3°) Explique rápidamente en qué consisten las diferentes dificultades de organización. (10 minutos- 7 a 8 líneas- 4 puntos)

4°) El artículo menciona unos problemas materiales que afectan el Museo del Prado. Trate usted de explicar en qué pueden perjudicar a España y al patrimonio cultural mundial también (10 minutos- 7 a 8 líneas- 4 puntos)

5°) A nivel personal, ¿cómo percibe usted el Arte y la difusión cultural? ¿Le parece importante preservar el patrimonio cultural? ¿Por qué? Trate usted de explicar cómo ha de organizarse la política cultural. (A nivel nacional, cooperación internacional, sponsoring, participación de ONG…)
(20 minutos- 12 a 15 líneas- 6 puntos)

N.B.

La última pregunta requiere una auténtica reflexión personal así como una explicación justificada de las afirmaciones.

Antes de entregar la copia es indispensable valerse de algún tiempo para volver a leer atentamente lo que haya escrito. (10 minutos)

¡Ánimo!

(Les temps indiqués entre parenthèses sont indicatifs et ont pour objectif d’aider le candidat à gérer son temps de façon optimale)

Según el artículo publicado en:

ABC Madrid 16 de septiembre de 2018

La exposición conmemorativa será inaugurada el 19 de noviembre por los Reyes, abriendo con ello el programa de actos, que se extenderá durante un año

Según el artículo de Natividad PULIDO

Aunque el director del Prado, Miguel FALOMIR, lo niega, el bicentenario del Museo del Prado no ha comenzado con muy buen pie que digamos. Se han conocido sendos informes técnicos que afectan a la salud de la pinacoteca. Por un lado, las grietas y humedades provocadas por las aguas subterráneas que pasan bajo el museo, que aconsejan crear nuevos pozos de drenaje. Por otro, las lesiones en las fachadas (…), con riesgo de desprendimientos, que han provocado unas obras de emergencia que durarán 16 meses y tendrán un coste de 4 millones de euros. El Prado tendrá andamios durante todo el bicentenario. «Nos gustaría no tenerlos. Pero un cuerpo de 200 años no es uno de 18. Lleva aparejados problemas. Tenemos que vigilar y tomar las medidas oportunas para que todo esté controlado», advierte FALOMIR. El ministro de Cultura, José GUIRAO, añade que «se ha intervenido en la fachada cuando los técnicos han dicho que había que hacerlo. Lo primero es la seguridad de las personas».

A ello hay que sumar el retraso en las obras del Salón de Reinos: tan solo se pudo aprobar en los Presupuestos Generales del Estado de 2018 una partida de un millón de euros, pero los trabajos no pueden comenzar hasta que se apruebe una partida extra en los de 2019. Y, además, se canceló la que iba a ser originariamente la exposición conmemorativa del bicentenario: «Circa 1819», comisariada por Javier BARÓN y Félix de AZÚA. Fue sustituida por otro proyecto, «Museo del Prado 1819-2019. Un lugar de memoria», comisariado por Javier PORTÚS. FALOMIR ya advirtió en su día que el cambio se debió a que el Louvre no concedió unos préstamos de importantes obras de Delacroix que iban a venir al Prado a cambio de unos Goyas. Pero la pinacoteca parisina canceló su muestra de Goya y los Delacroix ponían rumbo a Estados Unidos. Hay quien piensa que aquella exposición no era la más adecuada para celebrar los 200 años del Prado.

Sean cuales fueren los motivos del cambio, «Museo del Prado 1819-2019. Un lugar de memoria» sí contará la formación de la pinacoteca a través de sus donaciones y adquisiciones, pero también se pondrá el acento en la importancia del Prado en el desarrollo del arte contemporáneo. De ahí que incluya obras de los siglos XIX y el XX de Manet, Renoir, Sargent, Picasso, Miró, Gris, Saura, Motherwell, Pollock... Será inaugurada el próximo 19 de noviembre por los Reyes, dando así por abiertos los actos del bicentenario, que se extenderán durante un año, hasta el 19 de noviembre de 2019, día en que se conmemorarán los 200 años de la apertura al público del Real Museo de Pintura y Escultura. Se cerrará el bicentenario con la mayor muestra de dibujos de Goya jamás realizada.